INSTITUTE FOR DEFENSE ANALYSES

Summary of the Review of the National Information Assurance Partnership (NIAP)

Gregory N. Larsen, *Task Leader*

J. Katharine Burton
Patricia A. Cohen
Rick A. Harvey
Reginald N. Meeson
Michael S. Nash
Sarah H. Nash
Edward A. Schneider
William R. Simpson
Martin R. Stytz
David A. Wheeler

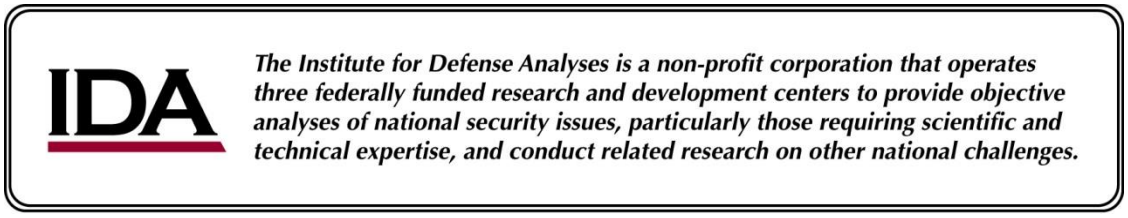
January 2006

IDA Paper
P-5224

Log: H15-000011

Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882



About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, Task BC-5-2382, for the OASD/NII DIAP. This study was mandated by the National Strategy to Secure Cyberspace which requires the Federal Government to conduct a comprehensive review of the National Information Assurance Partnership (NIAP) to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. The NIAP is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide technical leadership in the research and development of security-related information technology test methods and assurance techniques. The study reviewed the policy and requirements for cybersecurity, the current structure and functionality of the NIAP, and the expectations of the stakeholders. The study developed issues and recommendations and provided several options for pursuing cybersecurity programs that include all the elements necessary to establish an efficient and functional operational capability to strengthen the security of the software used in U.S. systems and commercial software products. The publication of this IDA paper does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

Copyright Notice

Summary of the Review of the National Information Assurance Partnership (NIAP)

Gregory N. Larsen, *Task Leader*

J. Katharine Burton
Patricia A. Cohen
Rick A. Harvey
Reginald N. Meeson
Michael S. Nash
Sarah H. Nash
Edward A. Schneider
William R. Simpson
Martin R. Stytz
David A. Wheeler

Summary of the Review of the National Information Assurance Partnership (NIAP)

This document is an edited summary of a paper (IDA Paper P-4009, Review of the National Information Assurance Partnership (NIAP)), originally prepared for the Assistant Secretary for Defense for Networks and Information Integration, (ASD-NII) in cooperation with the Department of Homeland Security (DHS). The work was performed under the task order, National Information Assurance Partnership (NIAP) Review. The summary has been modified from the original text in that funding details no longer pertinent have been deleted; format, grammar and spelling have been corrected; and some details have been shortened in their presentation. There is no intent to revise the original material, and all original findings are intact.

Contents

Figures

Tables

Executive Summary

The National Information Assurance Partnership (NIAP) is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to develop and promote technically sound requirements and methods for evaluating information technology (IT) products and system security. The long-term goal of the NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, the NIAP seeks to:

- Promote the development and use of evaluated IT products and systems;
- Champion the development and use of national and international standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the United States.

The President's *National Strategy to Secure Cyberspace* required the Federal Government to conduct a comprehensive review of the NIAP to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. The Department of Defense (DoD) and the Department of Homeland Security (DHS) tasked the Institute for Defense Analyses (IDA) on behalf of the Federal Government to consider the results of current policy and practices, the general efficacy and adequacy of current capabilities, and the subsequent affordability and viability of expanding the NIAP program to all Federal agencies. The direction was to:

- Characterize the NIAP intent and future expectations, conduct fact finding, and develop issues;
- Assess the impacts of selected issues and generate alternatives and options to address these issues;
- Analyze selected issues and options; and
- Recommend option(s) and an implementation roadmap.

Scope and Approach of Review

To ensure coverage of all relevant issues, the scope of this review included both the NIAP as it is currently instituted and the broader context of cybersecurity within which the NIAP operates.

IDA approached the NIAP review from three basic analysis viewpoints. Since Federal and agency policies ultimately dictate requirements, one team explored policies to determine what the NIAP has been directed to be. A second team examined current NIAP processes in order to observe what the NIAP currently is. A third team delved into the expectations of the various NIAP stakeholder groups to learn what users expect and need. This was done through interviews, an open forum, and a notice in the *Federal Register* soliciting comments on the NIAP. The results were then combined and synthesized by the entire project team to reach the conclusions herein.

This task was not intended to establish a baseline of detailed costs and specific benefits or to determine the statistical significance of any particular measure of effectiveness. Rather the effort was a review of the current posture of the NIAP relative to policies, guidelines, and standards; relative to the original intent of the partnership and current practices; and relative to a broad stakeholder set of expectations and experiences.

The review acquired as much specific data on actual benefits and costs as possible; however, the reviewers were not able to acquire enough evidence for a rigorous business case argument.

Findings Summary

The review organized its findings along the dimensions of the policies, practices, and expectations used to obtain information and to assess issues. The body of the report preserves the individual details of these findings. A synopsis of the report provides an intermediate level of detail following this executive summary.

This review affirmed confusion over the NIAP's role and scope in a cybersecurity context. Misunderstandings spanned five basic areas of characterization.

- Products claiming security features, functions, or properties (input to the NIAP);
- Evaluation processes for products with security features, functions, or properties (NIAP value-adding activities);
- Implemented systems incorporating evaluated products and non-evaluated products (use of NIAP evaluations);
- Operational outcomes or effectiveness of systems with security expectations from using evaluated products (outcome/benefit measurement versus NIAP input/output measurement); and
- Equipment, software, and expertise to perform evaluations and their limitations in determining security features, functions, or properties of products against

standards and in operational use (evaluation tools, techniques and infrastructure).

The overall findings in each area are summarized as follows.

Policy and Policy-Related Summary

The review identified and examined over 100 relevant cybersecurity-related policy and guidance documents. Three major documents provide the governing policies for NIAP and NIAP-specific evaluations. The remaining documents establish the cybersecurity environment in which the NIAP operates.

The cybersecurity policy landscape is complex. Although product developers and experts find it complex, they are better equipped to know and judge whether they are compliant, capable of conducting product security evaluations, and the utility of product evaluations in the larger environment of cybersecurity. For users and consumers of products claiming security properties and promoting security features, it's a much more difficult endeavor to know and appreciate whether a NIAP evaluation is valuable or meaningful in the environments or configurations in which they are incorporated or used.

Practice and Practice-Related Summary

NIAP activities as originally scoped remain valid. Little was discovered against the general proposition of testing and evaluating products against established standards for security properties. However, NIAP expenditure priorities versus the original scope of activities (e.g., evaluations, education training and awareness, and research and tools) have shifted and been dominated by increasing demands for evaluations with a corresponding declining budget for other NIAP activities.

NIAP as designed and implemented is incomplete to fully address the myriad issues and demands of cybersecurity emerging today. However, NIAP is accomplishing a major portion of its original goals with limited funding, but funding limitations put its immediate future in jeopardy. This limited funding has led to deficiencies in the NIAP relative to Protection Profiles, strengthening and fixing Common Criteria (CC) and requirements, development of tools for evaluations, and adequate linkage with certification and accreditation (C&A) processes.

Expectations and Expectations-Related Summary

Expectations of what NIAP can accomplish relative to the totality of cybersecurity demands – both actual and emerging needs – are not well understood and are often based on incorrect perceptions of what the NIAP is, what policies govern the NIAP, what the NIAP does, and varied experiences with security evaluations in contexts that may or may not engage with the NIAP. With an environment demanding more cybersecurity, competing ideas arise for what the NIAP could or should be contributing. No reliable

evidence was found that alternatives to the concept of the NIAP were sufficiently mature to be competing alternatives. That is to say, evidence was not collected that some response other than the NIAP was clearly and measurably better. However, many ideas on ways to improve the results and practices of the NIAP surfaced. A number of these expectations expressed by stakeholders or benefactors led naturally to the development of a number of options for improving the NIAP within the cybersecurity context. These options spanned all expectations expressed by the community. On one end of the spectrum of opinion, some thought there was no need for the NIAP and it should be eliminated. The other extreme expressed a need to move to a "new paradigm" to accomplish cybersecurity evaluations. This review found that the likely reality for the NIAP, when all comments were examined, was intermediate to these endpoints.

The review examined over 750 individual comments to identify major areas of issues and specific perceptions and expectations. The major areas of issues are education of stakeholders, research to obtain adequate tools for evaluation and alternate forms of assurance, applicability to critical infrastructure and their associated information systems, questions of product evaluation/assurance in relationship to process evaluation/assurance, and composition of products (both evaluated and unevaluated) into secure systems.

Recommendations Summary

The review explored six options in response to the findings in policy, practice, and expectations. The implications of these options were developed and organized as follows.

1. Eliminate the NIAP and product evaluations;
2. Continue the NIAP in its current form (reduced from the original intent);
3. Restore the NIAP to the original intent of the Letter of Partnership between NSA and NIST;
4. Modernize the approach to cybersecurity evaluations to reflect changes in the environment since its creation in 1998;
5. Take an integrated approach to cybersecurity evaluations; and
6. Take a forward-looking approach to cybersecurity evaluations (new paradigm).

These options were constructed to enable each (beginning with Option 2) to build on the prior option in terms of implementation increments. Option 1 was developed as a response to the expectation that the NIAP could be eliminated without replacement. Option 6 was developed as a response to the expectation that a totally new paradigm was needed for cybersecurity evaluations.

The report recommends the selection of Option 3, restoring NIAP to its original intent. Option 2 is required to achieve Option 3, but Option 2 addresses only the increasing demands for evaluations without regard to the original scope of the

partnership. Option 3 was designed as a response that restores the NIAP to its original scope, but within the context of the cybersecurity demands of 2005. Options 4 and 5 were further developed to expand and extend the scope of the NIAP for integration with existing C&A activities of information assurance (IA) and to extend this integration to the potential (but not yet proven) needs of cybersecurity.

NSA and NIST provided specific cost estimates to implement Options 2 and 3. These estimates, included in a separable annex to the original report, are closely matched to the relative estimates this review developed for implementing the options. The review established a baseline by using an existing budget and the quantity of evaluations performed for the budget. This was then used to estimate the incremental need for resources assuming growth projections for evaluation demands, and separate estimators were used to develop resource sizing for Options 3 and beyond. The following synopsis provides intermediate details of the recommendations associated with choosing to implement Options 2 and 3 going forward.

Conclusions

The review of the NIAP concludes:

- The NIAP is providing a useful and significant service;
- The purpose of the NIAP is neither widely or well understood;
- The NIAP is complementary to and supplements C&A; it is not a replacement for C&A;
- The NIAP needs to be better connected to and integrated with C&A;
- The NIAP should provide better information for system integrators, system engineers, and security engineers; and
- The NIAP should be established as an accountable program with distinct budget lines and supporting research.

The next section provides a synopsis of the report details for those readers seeking an intermediate description of the review. The remainder of the document provides the details discovered or developed during the review.

Report Synopsis

The National Information Assurance Partnership (NIAP) is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to develop and promote technically sound requirements for, and methods for evaluating, information technology (IT) product and system security. The long-term goal of the NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, the NIAP seeks to:

- Promote the development and use of evaluated IT products and systems;
- Champion the development and use of national and international standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the United States.

The National Strategy to Secure Cyberspace required the Federal Government to conduct a comprehensive review of the NIAP to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. The Department of Defense (DoD) and the Department of Homeland Security (DHS) tasked the Institute for Defense Analyses (IDA) on behalf of the Federal Government to consider the results of current policy and practices, the general efficacy and adequacy of current capabilities, and the subsequent affordability and viability of expanding the NIAP program to all Federal agencies. The direction was to:

- Characterize the NIAP intent and future expectations, conduct fact finding, and develop issues;
- Assess impacts of selected issues and generate alternatives and options to address these issues;
- Analyze selected issues and options; and
- Recommend option(s) and an implementation roadmap.

To ensure coverage of all relevant issues, the scope of this review included both the NIAP as it is currently instituted and the broader context of cybersecurity within which NIAP operates.

IDA approached the NIAP review from three basic analysis viewpoints. Since Federal and agency policies ultimately dictate requirements, one team explored policies to determine what the NIAP has been directed to be. A second team examined current NIAP processes in order to observe what the NIAP currently is. A third team delved into the expectations of various NIAP stakeholder groups to learn what users expect and need. This was done through interviews, an open forum, and a notice in the *Federal Register* soliciting comments on the NIAP. The results were then combined and synthesized by the entire project team to reach the conclusions herein.

This task was not a rigorous study meant to establish a baseline of costs and specific benefits or to determine the statistical significance of any particular measure of effectiveness. Rather the effort was a review of the current posture of the NIAP relative to policies, guidelines, and standards; relative to the original intent of the partnership and current practices; and relative to a broad stakeholder set of expectations and experiences.

The review attempted to acquire as much specific data on actual benefits and costs as possible; however, it was not able to acquire enough evidence for a business case argument. This should not be perceived as negative with respect to the value stakeholders perceive for a product security evaluation capability, but rather an inherent difficulty of obtaining the necessary data and its correlation with the effectiveness of resource execution.

Findings Summary

The review organized its findings according to the independent reviews of the policies, practices, and expectations the teams used to obtain information and to assess the issues of each area. The body of this report provides the individual details, some of which are not covered in this synopsis, as they are specific to a sub-category of the major areas explored.

Policy and Policy-Related (See Chapter 3)

Policies, guidance, standards, plans, and directions provided the basis for examining the environment of the NIAP and NIAP-specific roles and responsibilities, and the basis for judging NIAP performance. After examining this landscape, the policy review team established and organized findings into five themes: (1) cybersecurity, (2) standards, (3) research, (4) education, training, and awareness, and (5) acquisition. These permitted an assessment of the situation relative to the environment (cybersecurity); an established baseline of requirements (standards); the evolving nature of tools and products (research); the knowledge of users, developers, and other stakeholders (education, training and

awareness (ET&A)); and finally the constraining factors that enable or impede the effectiveness of product evaluations (acquisition).

Cybersecurity:

- The complex policy landscape and lack of a single source for current and superseded policies makes it difficult for Federal departments and agencies to determine the requirements for their particular situations.
- The NIAP was created by agreement between two agencies in different Federal departments, with no formal recognition by the Office of Management and Budget (OMB) or Congress. It has no official standing other than the agreement, which can be modified, rescinded, or terminated unilaterally by either of the two parent agencies.
- The NIAP's budget is not a line item in either parent agency's budget, preventing detailed oversight of the budget process to determine sufficiency and justification. This has resulted in decreasing available resources as the parent agencies address more pressing issues.

Standards:

- The National Technology Transfer and Advancement Act (NTTAA) 1995 requires the use of voluntary consensus standards in lieu of developing Federal standards. Federal agencies' determination of which standards to use requires mapping existing voluntary consensus standards, Federal standards (Federal Information Processing Standards (FIPS)), and standards from the different communities of interest to determine gaps, conflicts, and overlaps. To date, this mapping has not been done, or if it has, it was not evident to the researchers in this review.
- The existence of the communities of interest results in differing sets of potentially conflicting and non-interoperable requirements. While FIPS issued by NIST are mandatory for the Federal Government, national security systems (NSS) are exempt from them. NSSs have their own standards and guidelines, as do DoD and the Intelligence Community. Annex D provides more detail on the standards for these communities of interest.

Research:

- Current levels of cybersecurity research funding are inadequate and fail to address current cybersecurity issues, much less those of the future (such as grid computing, distributed intelligent agent systems, distributed knowledge management, composable systems, and systems of systems.)
- A timeline, schedule, and process for addressing future cybersecurity concerns are lacking.
- A process for coordinating government efforts and allocating research resources for cybersecurity research is lacking.

- The memorandum establishing the NIAP says that the NIAP seeks to foster research and development in security tests, methods, and metrics, but to date this has not happened.
- While some portion of information security research advances achieved as a result of the Homeland Security Act of 2002 may be of use for the NIAP, no process is in place to identify those results or to transfer them into the Common Criteria Evaluation and Validation Scheme (CCEVS) process.
- The need for research to improve the quality of our cyber defense and defensive information operations is widely acknowledged in numerous government documents; however, no document points to the NIAP as a tool for addressing this need or directs research that would result in the NIAP being able to address this need. In the few cases where the need for research is identified in a document, it is usually cited in relation to a specific threat, such as mobile malicious code, and never addressed toward improving the capability of determining if software is secure via the NIAP process.
- While the Clinger-Cohen Act imposes a research duty upon the National Science Foundation (NSF), there is no mechanism for communicating the NIAP's needs to the National Science Foundation (NSF) or for extracting NSF research advances and employing them for NIAP purposes.

Education, Training & Awareness (ET&A):

- The training documentation produced by NIST for the Federal Government (SP800-16) in 1998 was issued concurrently with the establishment of the NIAP. Although a model program when it was issued, the changes in policy, technology, management of Federal IT organizations, and organization require a similar significant update to this document.
- The level of detail in the current NIST SP800-16 is insufficient to ensure an appropriate level of knowledge for either the NIAP certificate users or certifiers. This detail is necessary for performance and evaluation of performance for those functions.

Acquisition:

- While the Federal Information Security Act (FISMA) documents specify the security controls that must be implemented in Federal unclassified systems, there is no requirement on how Federal agencies must choose those products. The requirement for acquisition of evaluated information assurance (IA) and IA-related products only exists for the NSS and DoD. Outside of this, no acquisition policy concerning IA/IA-related products exists for Federal departments and agencies since the Federal Information Resources Management Regulations (FIRMR) were rescinded in 1996. This means that the rest of the Federal Government can choose security products based on their own criteria that may or may not have been evaluated.

- The NIAP process leading to product certification does not directly contribute to systems certification required by statute and OMB.

Practice and Practice-Related (See Chapter 4)

The practices team principally found that NIAP is underperforming relative to original intent due to two driving factors. One is a shortage of resources to accomplish to the fullest degree all that was intended by the original letter of partnership. The second factor is that for a given level of resources applicable for the scope of original intent, these are rapidly consumed just meeting the non-discretionary requirements, leaving little for the remaining scope of NIAP intentions. Simply, other priorities are crowded out by the increasing quantities of evaluations, and thus the resources available must be applied to a very narrow portion of the original intent.

- NSA and NIST, without separate funding earmarked for the NIAP, have produced a flexible, capably staffed, although under-funded, product evaluation system.
- Budgeting restrictions have prevented the NIAP from developing education and training resources for IT system consumers, tools to support secure product development, and protection profiles for non-military applications.
- Oversight of evaluations has been limited due to stretched NIAP budgets and a shortage of qualified validators. The oversight mechanism meant to ensure that evaluations conform uniformly to all Common Criteria (CC) requirements is under-funded. The NIAP has made adjustments in both organization and resources. The current number of evaluations stresses the limits of the validation resources, and the number of evaluations continues to grow.
- Evaluations take longer than anticipated. Evaluation schedules are often extended beyond their original plan.
- Evaluations frequently result in modified products or claims. Most evaluations take longer than anticipated either because the product does not satisfy the initial claims or because the documentation is not adequate. The result is that either the product or the claims must be modified. This is actually a good thing if one ascribes to the "truth in advertising" approach, and reduction of claims in marketing materials would follow. However, sufficient data gathering has not been done to adequately quantify this effect. It appears (from experienced evaluators and validators) that the evaluation documents are the primary place that claims are reduced. Ideally, the product would be modified to meet the claims, but it is usually easier to obtain a certificate by reducing claims. The NIAP is working to have claim adjustments documented, but this only helps sophisticated customers who read it. When conformance to a protection profile (PP) is cited or required, the claims in the security target (ST) cannot be reduced below those of the PP. DoD requirements for PP conformance should be continued.

- Developers produce large amounts of data relevant to evaluations during their development and testing. Only a small portion of this data is provided to evaluators in the form of evidence. Consumers typically see only the product's evaluation certificate, which contains no vulnerability information, and the other information available to them is written in precise evaluation language, and typically includes little about residual vulnerabilities. The Education, Training, and Awareness (ETA) have lagged, so consumers are generally not well educated in reading the evaluation reports.

Expectations and Expectations-Related (See Chapter 5)

By far, this team had the most difficulty in developing a coherent picture of expectations. The objective was to gather as much information as possible concerning various opinions, experiences, and expectations for the NIAP in the context of cybersecurity, IA, and product evaluations. Every attempt was made to solicit any viewpoint without judgment of its validity. Instead, the review effort collated the many comments and inputs into stakeholder views, and organized the comments into 16 topical areas of coverage. This effort resulted in many observations that clearly may not be as important as the same observation provided some multiple of times.

The stakeholder views were categorized as:

- **Department of Defense (DoD) –** Individuals in DoD who represent the assured information system customer base;
- **Federal Government (FEDNonDoD) –** Individuals outside of DoD but in the Federal government who represent the customer base (such as the National Aeronautics and Space Administration (NASA) or the Federal Aviation Administration (FAA));
- **Process –** Individuals who are or have been involved in executing the current NIAP process, including validators and lab personnel, as well as NIST and NSA personnel;
- **Producers (Large and Small) –** Developers of IA or IA-enabled software that may be subjected to evaluation requirements, including large-scale producers such as Microsoft, IBM, and Oracle, as well as small business concerns;
- **Governance –** Individuals who are instrumental in making policy and mandating requirements for their agencies, such as heads of NSA, the NIAP, and Federal agencies;
- **Defense Critical –** Individuals who are involved with the operational capabilities of the commands of the armed services – as separate from branches of government such as NASA, FAA, etc.; and
- **Intelligence –** Individuals who are involved in intelligence gathering activities.

The results from the participants in the collection process were summarized by the team into those that clearly represented a stakeholder expectation for product evaluations

and/or the NIAP and those that were only an expression of experience with no further elaboration of whether that was intended to be interpreted as some kind of expectation.

The resulting topical areas used to organize the inputs into simple observational groups and expectations were the following. The summary findings from these detailed observations and synthesis of expectations are subordinate to each topical heading. In some cases, although the topic was mentioned frequently, no substantial finding was made by this review.

Consumer knowledge and understanding of evaluations

- Consumers need a better understanding of information assurance threats and protection methods, and a basic understanding of NIAP evaluation processes to interpret evaluation results and make informed decisions about product suitability for their needs.
- Evaluations are often reported in technical CC terms and do not state in plain language what information assurance protection the product provides.

The meaning of a product evaluation certificate

- Evaluation certificates in general do not identify the degree of security provided by the product or do not provide example applications for which the product is suitable.

Protection profiles

- Protection profiles covering core information assurance capabilities for general use have not been developed. A number of protection profiles that address the higher levels of assurance for national security systems have been developed by NSA for use by that community. Protection profiles for capabilities that satisfy more modest assurance requirements have not been developed.

Evaluation personnel and evaluation laboratory issues

- Product evaluators come from a variety of disciplines, with varying levels of expertise. Although the NIAP checks that evaluation processes are followed correctly, no process has been established to ensure adequate training of evaluators and validators.
- Current conflict of interest rules, particularly those that allow laboratories to develop evidence and conduct evaluations on the same products, are open to potential abuse.

Testing of products in evaluations

- Automated tools can help standardize evaluation processes, perform more thorough product analyses, and reduce evaluation costs. No standard collection of automated security analysis tools has been developed or assembled to support evaluations.

- Both the Common Evaluation Method (CEM) and protection profiles often omit detailed testing requirements.
- No automated review of source code is required for evaluations at evaluation assurance level (EAL) 4 and below. For software products, the code represents a complete technical specification of the product's functionality, and it is much more revealing than the other design and implementation documentation that is considered in evaluations. Automated source code review could screen out many common security flaws that currently go undetected.

Alternative forms of assurance

- Alternative forms of assurance are not significant concerns for most stakeholder classes. Alternative forms of assurance, however, may reduce costs and could be useful at lower evaluation assurance levels. Several interviewees believed that alternative assurance methods are needed, especially to reduce costs (such as a "CC lite"). This is the case for organizations or situations that cannot afford to pay for evaluations, such as many small web applications, small businesses, and open source software (OSS) projects. Support for alternative assurance levels was strongest for use in lower assurance evaluations. Many believed that NIAP evaluation would be strengthened if the alternative assurance methods were used to supplement the NIAP evaluation, with System Security Engineering (SSE), Capability Maturity Model (CMM), and Capability Maturity Model Integration (CMMI) specifically mentioned as examples of alternative assurance methods. These assurance methods would augment (not replace) the current assurance methods.

Relationship between certification and accreditation (C&A) and product evaluation

- C&A of systems was considered essential by all stakeholder classes, and product evaluation should improve C&A.

Mutual recognition, commercial viability, and related issues

- NIAP has not addressed warranty or liability issues for evaluated products. No legal or business-case analyses on who might underwrite warranties for evaluated products was found, or what effect warranties might have in promoting adoption of evaluated products.
- Mutual Recognition is necessary.

Research areas

- A number of open research problems remain unaddressed, including assurance metrics and solutions to composability, among other security problems.

Target of evaluation (TOE) versus product evaluation

- A number of products have been evaluated in unusual configurations and environments that do not represent consumers' general use. These evaluations

do not provide sufficient information to determine how these products will perform in typical system configurations and normal use.

Assurance maintenance

- Evaluations should include both maintenance assurance and flaw remediation work packages.

Cost and time issues

- "Evaluation costs are too high and they take too long." These are common complaints, particularly from small businesses. The documentation generated for evaluations is partly responsible. Although no significant finding was made by this review, the comments and observations in this topical area were consistent with other findings of the review.

National Security Telecommunications and Information Systems Security Policy (NSTISSP)-11

- Comments regarding NSTISSP-11 are included for completeness in the body of this report; however, no significant findings were made. However, the expectations are consistent with other findings of the report, such as the need for protection profiles and issues related to perceived and actual costs incurred to comply.

Critical infrastructure

- No finding was made in this category. However, an expectation expressed by stakeholders from all classes was that the Critical Infrastructure Protection (CIP) community should be brought under the national security mandates. Most government departments and agencies that are part of CIP are already under the FISMA mandates. Including CIP under product evaluation and CC mandates may create an undue burden of cost.

Nefarious and malicious behavior in code

- Although there was little input on this subject, malicious code and backdoor access paths inserted during development have to be considered in any assurance arguments. Many of the interviewees felt uncomfortable discussing this area, and there was little written input. Nevertheless, tools for specification analysis, examining code and product execution, and managing configurations are often encountered in the literature as necessary for product evaluations if both security effectiveness and affordability are to be achieved.

Comments concerning NIST

- No finding is provided for this topic, but stakeholders noted that NIST involvement is minimal and decreasing.

For further elaboration of these findings, Section 5.4 of Chapter 5 summarizes the 756 recorded comments from the interviews, forum discussions, and other contributed

input. “Issues” in Chapter 5 presents the principal concerns raised by interviewees, forum participants, and other contributors. “Expectations” presents recommendations expressed by these sources.

Options for the Way Ahead

Analysis of the issues, findings, and conclusions led to the identification of six options for the NIAP, in increasing magnitude of change.

Option 1: ***Eliminate the NIAP and product evaluations***

Shift virtually all of the responsibility for information system security to system-level C&A. System C&A is necessary anyway, even with evaluated products, but it would no longer benefit from the NIAP’s vetting of component products. C&A of separate systems would duplicate the effort of vetting common components.

Option 2: ***Continue the NIAP in its current form (reduced from the original intent)***

Continue the informal partnership between NIST and NSA, and continue to monitor product evaluations and participate in Mutual Recognition Arrangement and CC improvement activities. Additional personnel would be needed to handle the growth of evaluations. Because of budget constraints, however, current NIAP activities do not include many of the research and development objectives outlined in its original charter.

Option 3: ***Restore the NIAP to the original intent of the Letter of Partnership between NSA and NIS***T

Restore the NIAP to the full functioning envisioned when the partnership was first established in 1998. Bolster the NIST–NSA memorandum of agreement with a more formal charter and assignment of responsibilities, and direct the agencies to provide adequate funding. Consider additional partners, for example a component from DHS. This option addresses many issues raised about current NIAP operations, but it does not address changes in the cybersecurity environment that have occurred since its inception.

Option 4: ***Modernize the approach to cybersecurity evaluations to reflect changes in the environment since its creation in 1998***

In addition to restoring the NIAP as described in Option 3, provide more stable funding in the form of a national budget line item and strengthen oversight of NIAP activities. Then update the NIAP’s processes to address changes in the cybersecurity environment. For example, many software vulnerabilities are caused by a relatively small set of common implementation errors, and many of these errors can be detected or countered by tools. Requiring use of approved software tools would reduce product evaluation costs and improve effectiveness. Vulnerability testing would be included in all evaluations, not just in those of high-end products.

Option 5: ***Integrated approach to cybersecurity evaluations***

Extend Option 4 to integrate product evaluations into the larger context of information system security. Rather than merely testing finished products in limited contexts, evaluations need insight into a product's original security objectives and assurance aspects of the development processes used to produce it. Complex products have wide ranges of possible configurations, only a small fraction of which are subjected to evaluation. Applications are similarly wide ranging, presenting a huge variety of possible environments and often requiring extensive configuration adjustments. Current product evaluations do not provide sufficient information for C&A analyses. Research is needed to fully integrate these cybersecurity components.

Option 6: ***Forward looking approach to cybersecurity evaluations (new paradigm)***

Move security evaluations to a new paradigm. This is not an incremental change that follows the progression already described, but a completely new way of thinking about the problem of cybersecurity. While it is not possible to describe this option and associated resource requirements in actionable detail without further study, several aspects of this option are clear at this time. The new paradigm must address future risks and vulnerabilities to systems. It must ensure that the security of a system is greater than that of the sum of its parts. It must also address issues related to changes in system ownership, rapid changes in system composition, changes in data ownership and location, changes in user expertise, and increasingly complex systems. In other words, the new paradigm must be as dynamic as the environment within which it must work.

Summary of Review Recommendations

A number of actions are recommended to converge on a responsive approach to product evaluations within an overall context of cybersecurity and information assurance, which is expected to be derived from a combination of Options 3 to 5, with Option 6 as a goal. Although the review recommends Option 3 as a minimum to resource and restore product evaluations to the original intent of the NIAP, this first requires adequate resources to accomplish Option 2, based on the rapidly increasing number of evaluations in the pipeline and the limited resource capacities of the NIAP partners to conduct the minimum of activities required. Although Options 4 and 5 may appear similar, they are in fact distinct. Option 4 is intended to maximize the benefits of evaluations against standards; whereas Option 5 is intended to add capabilities that would enable product evaluations against standards to be integrated with other processes and their assessment and evaluation methods, such as Certification and Accreditation (C&A), and Test and Evaluation (T&E) of systems and their operating environments and specific configurations. This review concludes that such an integration will be a significant challenge and will likely require significant investment that may not be provided to the NIAP, but it represents a point of interface for the NIAP and the cybersecurity operating

environment. Thus, at a minimum it could extend its charter to include such interactions as part of the larger cybersecurity/information assurance issues.

1. It is recommended that DoD continue to:
   - Develop Protection Profiles (PP) for DoD and National Security applications;
   - Require conformance to PPs, where they are available;
   - Require vulnerability testing for products at the lower evaluation levels; and
   - Include aspects of flaw remediation and assurance maintenance in PPs.
2. Specifically, it is also recommended that DoD:
   - Require product evaluations to include maintenance assurance and flaw remediation in accordance with the CC;
   - Support the full integration of product evaluation and C&A processes;
   - Support the development and use of software tools for vulnerability analyses;
   - Participate in an annual assessment and review of the nation's cybersecurity posture; and
   - Support the development of a lower-cost, alternative form of assurance for products at lower assurance levels.
3. It is recommended that DHS:
   - Collaborate with DoD on the initiatives above and support extensions of these efforts to all Federal and commercial IA products;
   - Support vulnerability testing of all products undergoing evaluation;
   - Support the development of a set of core functionality protection profiles for use by Federal departments and agencies, by critical infrastructure components, and by the commercial sector;
   - Support the use of core PPs, where applicable, to give product buyers confidence in the product's security functionality and suitability for use; and
   - Support the full integration product evaluation and C&A processes for Federal departments and agencies and critical infrastructure components.

Report Organization

This report provides a large amount of detailed information. Some suggestions for finding material of specific interest are offered at the end of Chapter 1, following the description of the report's organization.

1. Introduction

1.1 Background

The National Information Assurance Partnership (NIAP) is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide technical leadership in the research and development of security-related information technology (IT) test methods and assurance techniques. To quote from the letter that established the partnership [NIST/NSA1997]:

> Consumers, in both private and public sectors, need confidence and assurance in the products they use to secure valuable information. That confidence is bolstered when their products have been evaluated, tested, and certified by independent organizations. As security products change to stay ahead of evolving threats, so must the tests, methods, and metrics used to evaluate them. The NIAP will employ the latest techniques to develop specification-based tests, methods, and tools so that testing laboratories and certificate issuing organizations – as well as consumers and producers of information technology products – will have objective measures for evaluating quality and security.

In addition to boosting consumer confidence in information security products, a second goal of the NIAP is to enhance the United States' ability to gain international recognition and acceptance for U.S. products that help ensure the security of IT systems and networks. *The Terms of Reference* that forms the basis for the working relationship between the two organizations is found in [NIST/NSA1998].

Action/Recommendation 4-4 of *The National Strategy to Secure Cyberspace* [WH2003] requires the Federal Government to conduct a comprehensive review of the NIAP to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. This review will include lessons-learned from implementation of the Department of Defense's (DoD) July 2002 policy[1] requiring the acquisition of products reviewed under the NIAP or similar evaluation processes. DoD and the Department of Homeland Security (DHS) cooperated on the review. This report presents the results of that review. The Institute for Defense Analyses

[1] In January 2000, the Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC) issued National Information Assurance Acquisition Policy (NSTISSP No. 11). That policy directs, "by 1 July 2002, the acquisition of all commercial off-the-shelf (COTS) Information assurance (IA) and IA-enabled information technology (IT) products shall be limited only to those which have been evaluated and validated in accordance with criteria, schemes, or programs of the Common Criteria, the National Information Assurance Partnership (NIAP) evaluation and validation program, and the Federal Information Processing Standards (FIPS) validation program." [NST2003]

(IDA) conducted this review in the broadest of terms based on an initial set of questions provided by the Homeland Security Council (HSC) and after subsequent conversations with DoD (Assistant Secretary of Defense for Network and Information Integration/ Defense-wide Information Assurance Program (ASD/NII/DIAP)) and DHS (National Cyber Security Division (NCSD)) organizations cognizant of oversight issues surrounding product evaluations.

1.2 Security in Cyberspace

The National Strategy to Secure Cyberspace [WH2003], issued in February 2003, argues that the information technology revolution has quietly changed the way business and government operate. The U.S. increasingly relies on an interdependent network of information technology infrastructures called *cyberspace*. The security of cyberspace is essential to our economy and national security, as numerous recent cyber-attacks have demonstrated. Testing and certifying that commercial products and systems are free of known and applicable security vulnerabilities and weaknesses are an integral part of the strategy to secure cyberspace. Freedom from all security vulnerabilities and weakness is an impossible task with today's technology; however, relative freedom from known and applicable security vulnerabilities is achievable. The need for cybersecurity has been growing since 1970, often in spurts, with responses that vary to meet specific situations. Annex E provides an historical look at the timeline of events leading to the development of the NIAP and the associated National Policy regarding information assurance (IA). This policy covering cybersecurity, IA, and NIAP is a complex and exhaustive response to growing cybersecurity concerns, with well-intentioned approaches to cybersecurity but also generating an overlapping array of requirements and mandates. These will be discussed at length in Chapter 3.

1.3 NIAP Scope

The long-term goal of the NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, the NIAP seeks to:

- Promote the development and use of evaluated IT products and systems;
- Champion the development and use of standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the United States.

The NIAP has made progress in all of these with the exception of the third point, for at least the defense industry. Additionally, the NIAP has made adaptations or been forced to adjust activity emphasis to accommodate the changing pressures brought about by the complexities of cybersecurity while remaining within the bounds of a letter of partnership and funding constraints.

1.4 Evolution of NIAP

For over two decades, NIST and NSA have promoted security in commercial off-the-shelf IT products. These efforts focused initially on the government-sponsored Trusted Computer System Evaluation Criteria (TCSEC). Several factors during the past decade influenced the harmonizing of these evaluation criteria, leading up to the internationally accepted and standards-based Common Criteria (CC), International Organization for Standardization (ISO) International Standard 15408.

These factors included:

1. Development of similar IT security evaluations criteria by other nations;
2. Globalization of the IT product market;
3. Inclusion of security into middleware, applications, and network devices; and
4. Cost and time span of evaluations.

At the same time that the CC standard was being developed, NSA began the transition of its Trusted Product Evaluation Program to the private sector. This transition continues today under the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security.

The NIAP was initiated by an August 1997 agreement between NIST and NSA [NIST/NSA1997]. Almost a year later, NSA and NIST signed a Terms of Reference document [NIST/NSA1998] that included the statement that the agreement can be modified, rescinded, or terminated unilaterally. The Terms of Reference gives each organization an equal voice in all aspects of NIAP decision-making, including selection of the NIAP projects, allocation of the NIAP resources, oversight of contractor support, and technical direction. NIST and NSA designate Management Representatives (MR) to provide guidance, direction, and priorities to the NIAP. The MRs must jointly agree on activities designated as the NIAP projects. The Terms of Reference are silent on the subject of funding except to say,

> Recognizing that NIST and NSA will not have equality in the amount of discretionary resources applicable to NIAP, each organization will first look internally for resources and/or contractual vehicles to accomplish a given task. If necessary, it is agreed that one organization may transfer funds to the other organization for the purpose of supporting a specific […] NIAP tasking

[through] separate implementing agreements under the Economy Act (31 U.S.C. 1535).

1.5 Disclaimer

The analysis approach used analysts from a number of backgrounds and experiences in a team approach (a total of 11 analysts were used). This report documents their consensus. Several members have had and continue to have experience with the CCEVS validation program (two are currently validators under the CCEVS program). While the use of their expertise and understanding were valuable resources to the study, their inputs did not shape or determine the contents of this report. Their inputs were treated as valuable and experiential based, but identical to other inputs in reaching the consensus process.

1.6 Report Organization

The report has been developed for a variety of audiences ranging from experts in cybersecurity and product evaluation to top-level decision makers only briefly familiar with these concepts. As a result, some chapters contain great detail and others summarize issues. This report is organized as follows:

- Chapter 1 covers the background, introduction, and administrative items.
- Chapter 2 covers the scope and expectations of the study.
- Chapter 3 discusses the underlying policy basis in detail for the NIAP and the current state of policy implementation.
- Chapter 4 describes the NIAP and how it has evolved from its inception to its current organization and responsibilities.
- Chapter 5 summarizes the expectations of the stakeholders that were gleaned from interviews, solicited inputs, and literature search.
- Chapter 6 integrates the findings of Chapter 3, 4, and 5 and provides overall areas of concerns and approaches to some solutions, including the tradeoffs necessary to synthesize programs.
- Chapter 7 builds on Chapter 6 by providing approaches and options for the courses of action concerning the use of product evaluation in an overall cybersecurity framework.
- Chapter 8 provides the detailed actions necessary to implement the options of Chapter 7.

Detailed information, or information too voluminous to include in the body of this report, is provided in the Annexes as follows:

- Annex A contains the References and Bibliography.
- Annex B lists Acronyms.

- Annex C contains the Glossary.
- Annex D contains further policy information.
- Annex E provides NIAP historical data.
- Annex F discusses software tools for security analysis and proactive defense.
- Annex G discusses alternate forms of assurance.
- Other Annexes exist in the original report but have been eliminated from this summary.

The complexity of the subject and the depth of the analysis may dictate how this report is best used. For example, those who wish to know what options are available and what steps are required to implement them may wish to proceed directly to Chapters 7 and 8. Footnotes and cross-references will eventually take you to source data of interest. The individual who wants a level of detail beyond the executive summary may wish to read Chapters 1 and 2, and then skip to Chapter 6. Chapter 6 rolls up a number of details, with sufficient cross-reference to allow back-tracing to the text in Chapters 3 through 5. Most of the supporting data (although not all) has been provided in annexes to improve the flow.

2. Scope and Approach of Review

The National Strategy to Secure Cyberspace [WH2003] required the Federal Government to conduct a comprehensive review of the NIAP. The Review Tasking section below describes the scope and expectations of the task statement provided to IDA. The following sections discuss the terminology used in the report, identify communities of interest, and describe the review methodology.

2.1 Review of Tasking

For this review, DoD and DHS tasked IDA on behalf of the Federal Government to consider the results of current policy and practices, the general efficacy and adequacy of current capabilities, and the subsequent affordability and viability of expanding the NIAP program to all Federal agencies. The direction was:

1. Characterize the NIAP intent and future expectations, conduct fact finding, and develop issues;
2. Assess the impacts of selected issues and generate alternatives and options to address these issues;
3. Analyze selected issues and options; and
4. Recommend option(s) and an implementation roadmap.

The scope of this task covers government-wide issues, although particular emphasis is placed on DoD and DHS issues and concerns. This scope is broader than the NIAP as it currently exists. Findings and recommendations, therefore, may apply to other aspects of the cybersecurity problem not currently addressed by the NIAP. The options explored led to an integrated approach to a product-evaluation capability, without prejudice to who has responsibility for execution. The complexity of the issues, limited cost-benefit data, and options made it out-of-scope to provide detailed cost estimates after developing options. However, NSA and NIST provided estimates of cost to implement several of the options after reviewing them with IDA for clarification of possible ways ahead. Further effort is required to document and fully explore a rigorous analysis of alternatives or business case analysis for product evaluations within the surrounding context of cybersecurity and IA.

2.2 Methodology

The following describes the specific review approach.

The review team took a three-pronged approach to reviewing the NIAP (See Figure 1). Since Federal and agency policies ultimately dictate requirements, one team explored policy to determine the need, that is, what the NIAP must be. The policy review is documented in Chapter 3. A second team reverse-engineered the current NIAP process in order to make observations about practice, that is, what the NIAP currently is. The process review is documented in Chapter 4. A third team delved into the expectations of various NIAP stakeholder groups in order to find out what users expect and need. This was done through interviews, an open forum, and a notice in the Federal Register soliciting comments on the NIAP. The expectations review is documented in Chapter 5.

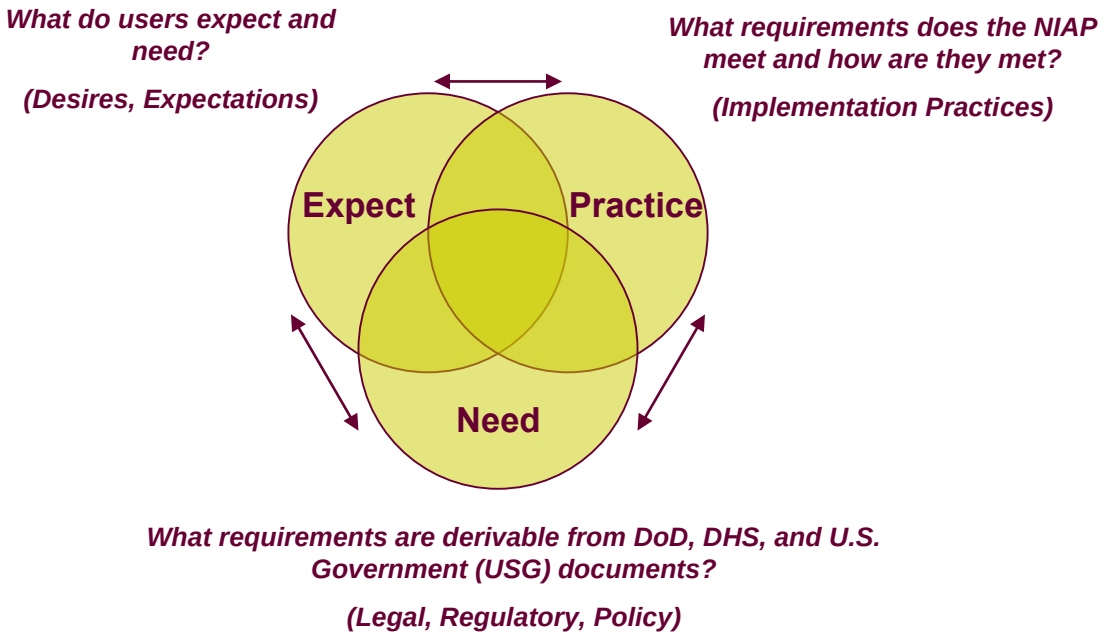


Figure 1. Three-Pronged Approach

Several common themes arose in each area of review. Results from the three areas are integrated into a complete perspective in Chapter 6. This combines the common findings and attempts to resolve apparent contradictions among requirements, process, and expectations. The teams then identified options for closing the gaps and analyzed each option for resources, feasibility, and time scale. Chapter 7 describes six options, along with their pros and cons. Chapter 8 is a roadmap of near-, mid-, and long-term actions to accomplish each option.

The scope of the review included the environment from which needs and expectations arise and into which NIAP performance results deliver benefits or consequences. The method above primarily deals with a characterization of the situation both external to the NIAP and within the partnership. The assessment of issues and

development of options and recommendations depends also on obtaining adequate data and information to indicate how well the NIAP is performing and relative to some baseline. One baseline is relative to itself. Another is relative to externally imposed metrics and measures of value. The following discussion is meant to provide a perspective on the notional data and information the review tried to obtain in order to provide a quantitative picture of the NIAP – its value and its costs. Such data was sparse, and the review was not able to acquire sufficient quantitative data to support strong cost-benefit arguments. However, the following background provides the basis that the review assumed could be characterized when it initiated its collection of data and assessment of performance and cost.

2.3 Background – Cybersecurity Landscape

Sufficient anecdotal evidence prior to the review and observations during the conduct of the review indicate the NIAP role is poorly understood. Also heard expressed were desires for the NIAP to be and do more than it actually does. Significantly, these perceptions set the stage for what the review affirmed. Namely, that cybersecurity issues generally were being confused with the NIAP – not by the NIAP, but certainly by users, and in some cases by those involved in related aspects of the NIAP. Before examining the NIAP and its role, an analogous example is provided to assist the reader. This analogy was frequently encountered during interviews with stakeholders and is presented only to establish an analogy (although imperfect) for separating NIAP roles/responsibilities from other cybersecurity roles and responsibilities.

The prior anecdotal evidence and the subsequent expectations comments affirmed that confusion and discussion of the NIAP role and scope in the cybersecurity context was shaped by misunderstanding of five basic areas that set the scope and boundaries for cybersecurity capabilities. These areas were generally the following, and the reader should keep this model in mind when reading the details of this report.

- Characterization of products claiming security features, functions, or properties (input to NIAP);
- Characterization of evaluation processes for products with security features, functions, or properties (NIAP value-adding activities);
- Characterization of implemented systems incorporating evaluated products and non-evaluated products (use of NIAP evaluations);
- Characterization of operational outcomes or effectiveness of systems with security expectations from using evaluated products (outcome/benefit measurement versus input/output measurement); and
- Characterization of equipment, software, and expertise to perform evaluations and their limitations in determining security features, functions, or properties of

products against standards and in operational use (evaluation tools, techniques, and infrastructure).

2.3.1 Physical Security Analogy

Consider the security of a house. In this example, the house is the system and the neighborhood is the environment. Security is provided by a set of products such as door locks, window locks, bars on the windows, broken-window detectors, motion sensors, and alarms. There are different types of locks and sensors, which would correspond to the algorithms in computer security systems. A five-tumbler lock may take more time to pick or force than a three-tumbler lock. Effective placement of these products depends on the layout of the house. In addition, effectiveness depends on the algorithms (five-tumbler locks versus three-tumbler) and how they are used: if someone does not set the alarm system, forced entry may not be detected until too late. In the end, alarms are tested, sensors are tested, and scenarios of break-ins are run against the system to be sure the risks are understood.

Note that security is not absolute. The amount of security in an information system is restricted by the value of the data: someone does not pay more for the security devices than the data being protected is worth. Also, security devices tend to make systems harder to use. Banks have lots of money and pay a lot for such things as vaults and armed guards; even so, they are occasionally robbed. The goods in a house typically are of much less value than the money in a bank. Most homes do not have alarm systems. These systems add cost to install and to provide monitoring; they also make entering and leaving the house more difficult since the alarm must be turned off and turned back on.

Some information security products implement an algorithm that differentiates the strength and usefulness of similar products. For example, while many operating systems authenticate users, some do so using passwords and others using smart cards. In a house, while all locks protect against unauthorized entry, some use a key to open, others a combination, and still others a garage door opener. The number of tumbler pins and physical keys are measures of protection strength. The door locks and physical keys are an analogy to passwords for strength of protection.

To evaluate the security of a house, one should start with the overall layout of the house and the placement of the various security products to see whether there are unguarded entry points or mismatches between products. Identified weaknesses should be tested to see whether they are exploitable. Also, an overall attack should be tried to determine whether there are unexpected weaknesses. If the same model lock is used on each door, however, one need not try to pick each of them: one is enough. Furthermore, if a laboratory has already tested the lock and determined that it properly incorporates some number of pins and that its case has a specified hardness, the strength of the lock does not

need to be tested at all at the house, but rather just that the lock has been properly installed.

Laboratory testing of individual security products such as locks and motion sensors corresponds to the NIAP's product evaluation function. Evaluating the security of a house that incorporates those products corresponds to another important function, Certification and Accreditation (C&A). After ensuring that the devices are installed and configured properly, C&A can rely on the laboratory's protection findings.

2.3.2 Cybersecurity Problem Decomposition

Figure 2 articulates a security evaluation framework in which the NIAP role, both current and as it may evolve, can be understood, and that can be used to understand the findings and conclusions of this review. Furthermore, this framework should help the reader of this report to separate "what the NIAP is," "what the NIAP does," and "what may be expected of the NIAP." It can also be used to determine what interfaces the NIAP has with other security evaluation processes. Figure 2 illustrates the framework as an "onion-skin" of successively increasing statements of security worthiness.

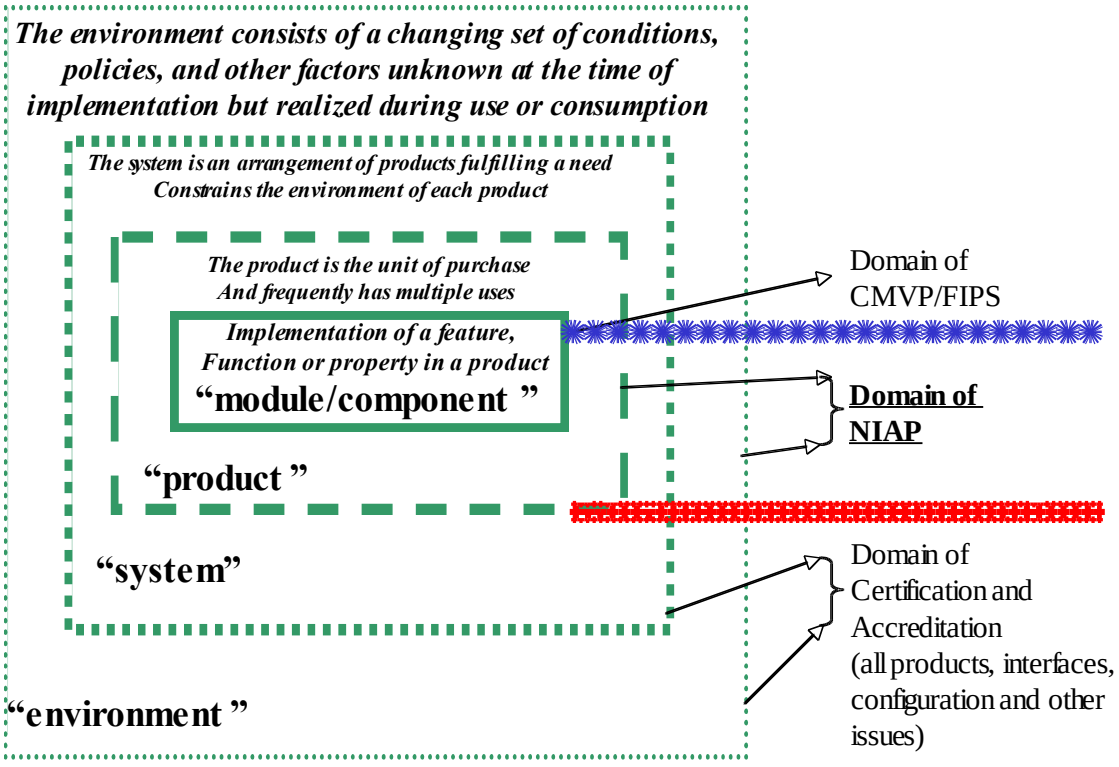


Figure 2. Framework of Cybersecurity Relationships

Information assurance or IA-enabled products contain functionality that supports confidentiality, integrity, authorization, availability, and other IA functions. However,

products that do not fit this category may very well have an impact on the security of systems. Those products, such as word processors, spreadsheets, financial utilities, etc., are not normally thought of as IA or IA-enabled, but they should nonetheless be candidates for vulnerability testing, which is discussed later. Ultimately, an organization should be concerned with its entire information infrastructure. This infrastructure consists of a system (the house in the analogy) of many nodes connected by physical and wireless networks. The system operates in an environment that is partially controlled and partially uncontrolled (the neighborhood in the analogy). Security is instituted to protect this system from the uncontrolled part of the environment.

In order to protect a system, an organization will rely on a variety of products, including devices such as firewalls, intrusion detection systems, and smart card readers (locks and sensors in the analogy). In addition, software that runs on system nodes, such as operating systems that identify users and limit access to files and browsers that provide secure communication to services, contribute. The security of the system depends on the products that are used, the specific security algorithms (such as cryptography) (these are mechanisms in the locks and sensors in the analogy), the way that they are incorporated into the system architecture (placement), and the way that they are used. The system developer does not solely rely on tested products but also tests his overall system through C&A, which is designed to quantify the risks inherent in the system as a whole. Since the products are tested individually, C&A can worry less about the product details and focus more on their arrangement, inter-relationships, and the end effect.

Evaluation of information systems is similar to that described for the house. Each system must be certified and accredited that its overall design does not have unacceptable weaknesses and that the various security products have been properly installed as spelled out in the DoD Information Technology Security and Certification Process (DITSCAP), Defense Information Assurance Certification and Accreditation Process (DIACAP), or National Information Assurance Certification and Accreditation Process (NIACAP). Individual security products are tested in laboratories to verify that they provide the stated security claims (Common Criteria Testing Laboratories (CCTL)). Other laboratories are used to verify that a product properly implements some algorithm or feature (Federal Information Processing (FIPS) laboratories). Because of the laboratory analysis done under FIPS, the NIAP evaluation does not need to examine algorithm or feature implementation (e.g., the strength of encryption between network nodes). Because of the evaluation done by the NIAP, the system certification does not need to do low-level testing of product-related security features (e.g., the strength of authentication at the administrator's console). The NIAP, as described in this report, focuses on the area between algorithm certification and system certification and accreditation. While the NIAP is currently restricted to IA or IA-enabled products, other products may be considered as potential sources of vulnerabilities.

2.3.3 Product Evaluation Business Case

It is assumed that product evaluation, used properly, is a positive contributor to the cybersecurity of systems. Properly executed product evaluation will reduce the burden of C&A and pay for itself by reuse in the many systems that use the product. Without product evaluation, the properties of the individual products are examined each time a C&A is done on a system that uses that product. These evaluations may be at different levels of sophistication, depending upon the expertise available to C&A. Product evaluation itself becomes more valuable when it provides useful, reusable information about products that can be integrated with C&A. Product evaluation becomes less valuable when its information is not useful or is obscure, unavailable, or not able to be integrated with system evaluations. Different users have differing senses of value depending on where they reside in the framework, what they are willing to risk, and what they can afford to pay for the value they desire. Various users and consumers of the NIAP bring differing senses of what the value-proposition means. At the system layer, a product evaluation has no meaning unless the product is configured and used in the same way as it was when evaluated. Also, the contribution of a product to the overall security value of a system depends on the placement of the product in the overall system architecture: putting a vault door on a house adds nothing if the windows are left open and unprotected. This inferred, and often unstated, view of what constitutes value creates both misunderstanding and confusion about what the NIAP is, does, and is expected to accomplish. There is an intrinsic assumption that building a house using specified and tested products will improve the overall worth of the house. The same is assumed for building a security system using specified and evaluated security products that use tested and evaluated algorithms.

2.3.4 Cybersecurity Landscape Summary

This framework sets the stage for the approach and methodology the review team undertook and the subsequent interpretation of the NIAP review results. The framework for this review and presentation of results can be portrayed in two dimensions of capability versus cost. The objective of the review was to collect quantitative evidence to judge NIAP efficacy (value-proposition) and affordability (cost-effectiveness); as might be expected the further up the "value-proposition-chain" one moves, the more difficult attaining quantifiable evidence of the security worthiness of and for a particular instance of a particular product implementation under constrained or unknown conditions of use becomes. This is further discussed in later sections of the document. Additionally, the complexity of presenting options makes the determination of precise costs beyond the scope of this analysis. Rough order of magnitude data will be provided, which is the best estimate (without analysis) of the individuals involved in the study. Once decisions are made on which options to pursue, it is recommended that the NIAP be asked to provide cost estimation.

2.4 Terminology

Information Assurance and *cybersecurity* are terms with established definitions. However, the terms are often used loosely and in contexts in which the established definitions are not widely understood or known − and the body of knowledge, skills, and technologies are even less well known by the user. Rapidly changing technology and a changing threat environment are largely responsible for the lack of stability in the use of terminology. Moreover, the meanings of terms such as *cybersecurity, computer security, network security, information security,* and *information assurance* change depending on who is using them and in what context. Annex C provides a glossary of terms. At the end of Annex C there is further background on several of the terms used in this report.

2.4.1 Nomenclature

The complexity of the subject of the NIAP in the context of the cyberspace landscape and the steps taken to improve overall cybersecurity necessitates a labeling convention for this report. In citing *Findings,* we use a tag [Fx-n], where *F* is for finding, *x* is one or more characters that provide reference to the analysis segment that generated the finding, and *n* is the number of findings of this type (for example FPCy-1 in Chapter 3 is the first Finding under Policy issues for Cybersecurity). Similarly, we have labeled *Observations* [Ox-n], *Assumptions* [Ax-n], *Conjectures* [Cx-n], *Expectations* [Ex-n], and *Recommendations* [Rx-n]. These tags are for reference to derived conclusions and act as an aid for traceability.

2.5 Communities of Interest

When describing the evaluation procedures for products and systems, a discussion of the various communities they pertain to is needed because different communities have different requirements. It is significant that the NIAP must serve all of these communities as well as the broader communities outside of the Federal Government, with a product certification process that will raise the basic security level of all of the participants in and out of government. The CC were designed for the broader community, and the U.S. component must serve that broader constituency. However, U.S. Government stakeholders often have differing requirements for and emphasis on product evaluation. This indicates that some level of consolidation, at least for process and evaluation methods, could reduce overall complexity. Figure 3 below shows the relationship between the various communities addressed by C&A standards: Federal Government, DoD, National Security, and Intelligence. The bottom cylinder consists of all departments and agencies in the executive, legislative, and judicial branches of the Federal Government. DoD, as one of the departments of the executive branch, is perched above. There is considerable overlap between DoD and the national security and intelligence communities positioned next to the DoD cylinder.

The national security community of the executive branch is an amalgam of institutions:

- Department of State (including our embassies and consulates, plus our overseas communications and foreign assistance programs);
- DoD (encompassing the armed forces and very large intelligence components);
- Central Intelligence Agency (CIA);
- DHS;
- Department of Justice (including the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration); and often
- Departments of Commerce, Treasury, and Energy.

At the top of the diagram is the Intelligence Community as established by Executive Order 12333, United States Intelligence Activities, consisting of the:

- CIA;
- NSA;
- Defense Intelligence Agency (DIA);
- Offices within the DoD for the collection of specialized national foreign intelligence through reconnaissance programs;
- Bureau of Intelligence and Research of the Department of State;
- Intelligence elements of the Army, Navy, Air Force, and Marine Corps, the FBI, the Department of the Treasury, and the Department of Energy; and
- Staff elements of the Director of Central Intelligence.

As these descriptions and the figure show, there is considerable overlap and some separation among the communities. Not shown is the commercial industry, parts of which are considered critical infrastructure, because although they are not stakeholders at this time, they do contribute to the overall cybersecurity posture. This further complicates the problem of policy and guidance, which will be discussed in the next chapter.

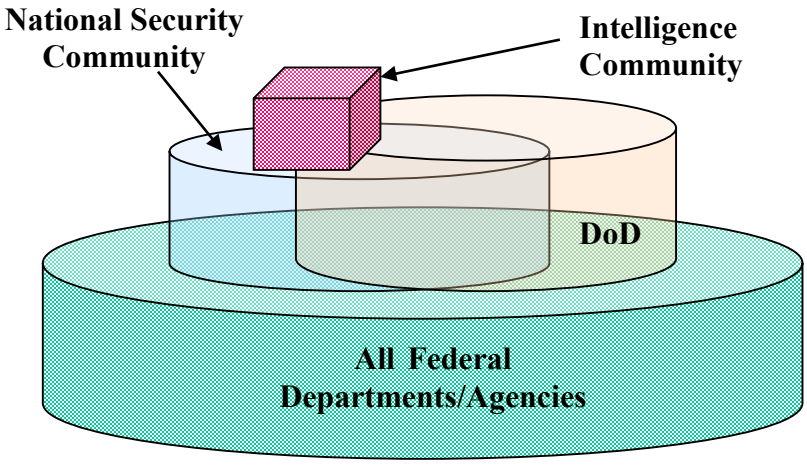


Figure 3. Communities of Interest

2.5.1 A Notional Performance Indicator/Cost Trade Space

Ultimately the need for improvements in any product or scheme must be based upon the performance cost trade space shown in Figure 4. The figure shows the trade space between cost and performance and the transitions that can be undertaken to either improve performance or reduce the price. Three such transitions are shown in the chart. The first is a transition to a lower operating performance curve, to reduce cost. Here, a decision to sacrifice performance (which may be above minimum thresholds) to reduce costs is made. A second transition is to make improvements in the current system with the trade being increased cost for increased performance. The third transition is to a higher-performance operating curve. In this case, a new approach and a demand for higher performance are being sought. The key is to have good data on both the performance and cost of the current operating environment so that estimates can be made for each of the transitions. The goal of this analysis is to provide trade space options. However, insufficient data was available to fully exercise this method of assessment to the degree necessary to make a fully informed business case for the outcome effectiveness of product evaluations versus alternatives and their potential costs. However, the paradigm below provided a basis for seeking such data from stakeholders. The notional performance/cost indicators shown below are input/output indicators to the NIAP. The review sought but did not discover sufficient and detailed data to apply this method of review to outcome effectiveness as a performance indicator nor costs of potential alternative capabilities. However, the notional method did help inform and structure the development of options for a way ahead.

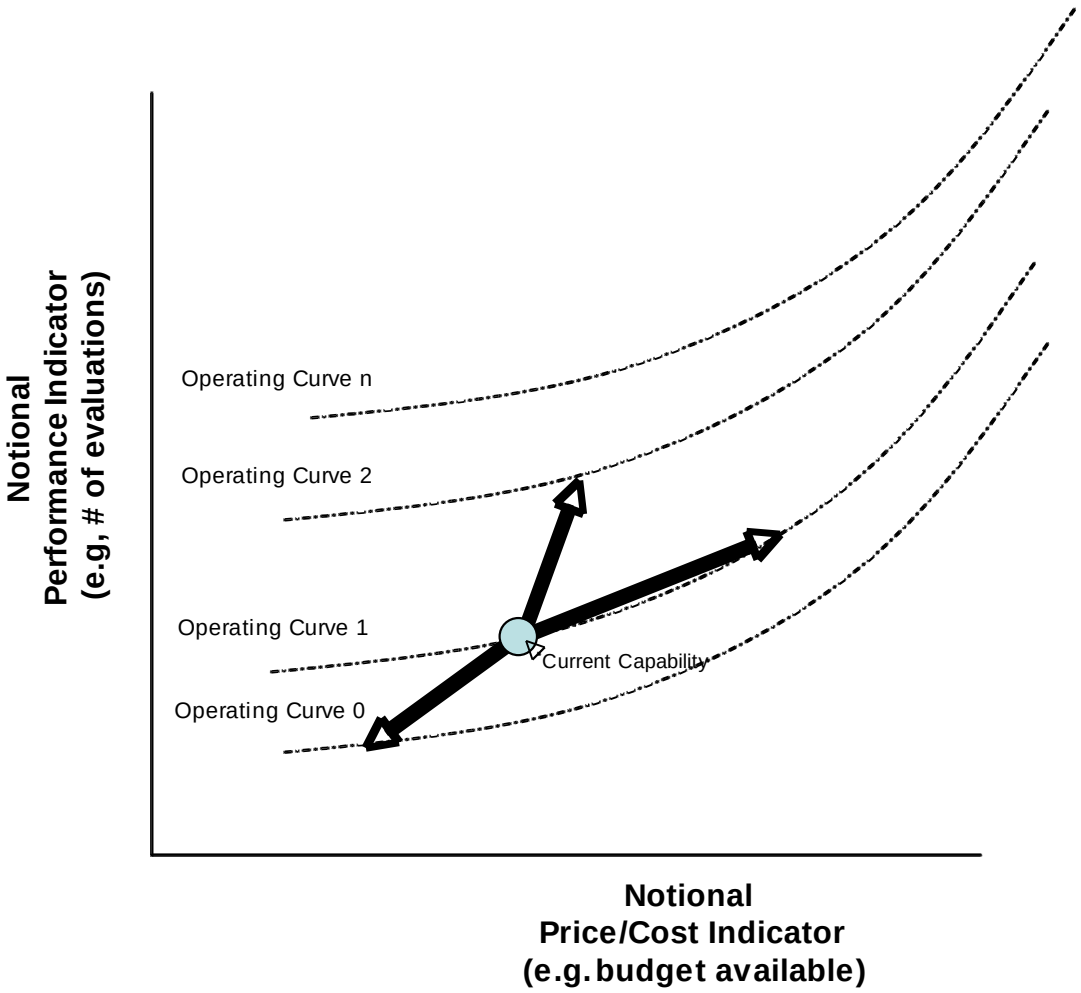


Figure 4. Notional Performance/Cost Trade Space

3. Policy Review

3.1 Scope and Context

This is the first in a set of three independent analyses of the cybersecurity landscape and the NIAP as it fits into that landscape. Since Federal and agency policies ultimately dictate requirements, IDA explored policy to determine what the NIAP must be. Policy and the strategies for implementing policy are found in several types of documents including:

- Federal statutes, Executive Orders, and Presidential Directives;
- Standards or department-level directives;
- Administration strategy documents; and
- Administration and congressional reports.

The first two types define official policy. They say what needs to be done and who is responsible for doing it, and they give some expectation of how it is to be done and whether there is a preferred method.

Administration strategy documents describe an administration's approach to implementing policy. Administration and congressional reports provide insight into the difficulties facing Federal departments by documenting progress (or lack thereof) in implementing policy.

Annex A lists the wide range of policy documents that we reviewed for their relevance to the NIAP process. Annex D contains detailed discussions of the relevant specifics of each document.

3.2 Themes

The discussion of requirements is organized around five themes that occur across policies:

1. Cybersecurity;
2. Standards;
3. Research;
4. Education, Training, and Awareness (ET&A); and
5. Acquisition.

Some policies contain requirements in each area; other policies focus specifically on a single theme. The relationships among the various policies are generally organized thematically and hierarchically. Analysis of these relationships provides a more understandable picture of the policy landscape. A section summarizing Findings and Recommendations for each theme concludes this chapter.

3.2.1 Cybersecurity Policies and NIAP

In this report, the terms *cybersecurity* and *information assurance* are used interchangeably because their definitions are quite similar. The term *cybersecurity* gained formal status when The Department of Homeland Security Authorization Act for Fiscal Year 2005 [DHS2005] amended the Paperwork Reduction Act to define it as:

> The prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The definition given in the National Information Systems Security (INFOSEC) Glossary [NST2000c] for information assurance is:

> Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Both cybersecurity and information assurance encompass the "five pillars" of information assurance – availability, integrity, authentication, confidentiality, and nonrepudiation of information systems as well as the concepts of protection and restoration. *Cybersecurity* refers explicitly to computers and electronic systems, whereas *information assurance* refers more broadly to information systems, which might or might not be electronic.

The NIAP is both an organization and a process created to address a specific requirement for cybersecurity for a specific community of interest. To the extent that it is successful, it contributes directly to the overall increase in security of national security systems (NSS), and indirectly contributes to Federal Government and private sector security products.

Chapter 1 described how the NIAP was created by agreement between NSA and NIST to assist both organizations in fulfilling their statutory cybersecurity responsibilities under PL 100-235 (Computer Security Act of 1987). Annex E provides a more complete history of the NIAP. Initial funding and staffing were provided per agreement by both organizations, with the understanding that the majority of future funding should come

from commercial testing laboratories conducting CC-based evaluations of IT products on a fee-for-service basis.

The expectation that the majority of the NIAP funding would be provided by the fees charged to companies undergoing the certification and validation process has failed to materialize. For one thing, government oversight is mandated in evaluations. This oversight is not paid by the evaluation itself, and increasing amounts of resources have been diverted to oversight of a growing evaluation program. Second, the National Voluntary Lab Accreditation Program (NVLAP – this program certifies CCEVS commercial laboratories) has the right to charge laboratories fees associated with their evaluation and certification under the CCEVS. However, the fees barely cover the costs accrued by NVLAP. Finally, the labs doing the certification do not provide funds for the other activities the NIAP was expected to support. At the same time, new statutes and priorities from both parent organizations have changed the mix of activities that can be supported, leaving little discretionary funding for activities like the NIAP. The result has been that the NIAP has shed functions that were not directly related to evaluation.

The Computer Security Division (CSD) is the division within NIST responsible for carrying out NIST's mandate in cybersecurity. The Federal Information Security Act (FISMA) requires an annual report from NIST on the status of its activities required by the statute.[2] In the 2003 report (the first one after FISMA went into effect), the CSD reported the current status of its activities and a statement that "…along with many other NIST units, [CSD] is taking a significant budget cut in 2004. The work planned for 2004, as described in this report… is very conditional. This budget cut will delay and curtail some of the planned work…."[3] The cuts mentioned limited NIST's participation in the NIAP to less than 1 staff year and in the NVLAP – the program that certifies commercial laboratories to do product evaluations. The decrease in budget for NIST is symptomatic of the shift in priority away from supporting the NIAP.

The Information and Security Privacy Advisory Board (ISPAB) completed a report on funding for the cybersecurity program at NIST and provided their findings to OMB. The details of the funding show an inconsistent level of funding, with some years showing a significant growth, and others a significant decrease, unrelated to tasking from Congress or the Office of Management and Budget (OMB). As the report states, the most recent "unfunded mandates" put a severe strain on NIST's ability to meet its commitments and expectations, including support for the NIAP. [4] Since the existence of

---

[2] FISMA, Sec 303, para (d)(10).

[3] NIST CSD, *2003 Annual Report "*Welcome" by Edward Roback, Division Chief, p. 2.

[4] ISPAB report, "A Report by the Information Security and Privacy Advisory Board," June 2004, Document is available at: http://csrc.nist.gov/ispab/bd-recommendations/ISPAB-ReportAdequateFundingNIST-CSD.pdf.

the NIAP is not a congressional or Federal requirement, the priority for support has fallen below other requirements, resulting in NIST's almost complete withdrawal from participation in the NIAP. The ISPAB strongly recommended that the NIAP be properly funded to address activities required for the Federal civilian sector and to ensure balance in the NIAP's activities.

In testimony before the House Committee on Government Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census on 16 March 2004, Deputy Under Secretary of Commerce for Technology, Benjamin H. Wu, laid out the activities NIST has accomplished since the enactment of FISMA, emphasizing the priorities and funding challenges facing NIST. The Commerce Department had requested a funding increase for FY05 to address these priorities, including that required for NIST's participation in the NIAP.[5]

OMB acknowledged the importance of the work that NIST does and reported on a number of NIST's activities in both the FY03 and FY04 FISMA Reports to Congress.[6] OMB included mention of NIST's participation in the NIAP but did not comment on either the priority or sufficiency of either that participation or any of NIST's activities.

The Cyber Security Industry Alliance (CSIA), a relatively new industry group, has taken on a number of issues in cybersecurity, one of which is the NIAP. It issued a report in July 2004 with a number of recommendations to improve the NIAP process, which will be discussed in a later chapter.[7] Later in 2004, CSIA issued its "Agenda for the Next Administration" and made specific recommendations concerning NIST funding and strengthening of the NIAP certification.[8]

NSA, whose budget goes through DoD, has historically been successful in obtaining funding for its various programs. However, the support provided to the NIAP is not identified in a specific line item that can be identified and monitored to determine its sufficiency. Nonetheless, funds have been provided to the NIAP for the execution of its

---

[5] Wu, Benjamin, "Statement Before the Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, U.S. House of Representatives," 16 March 2004. Document is available at: http://www.technology.gov/Testimony/BHW_040316.htm.

[6] OMB, "FY2003 Report to Congress on Federal Government Information Security Management," 1 March 2004. Document is available at: http://www.whitehouse.gov/omb/inforeg/fy03_fisma_report.pdf.

"FY2004 Report to Congress on Federal Government Information Security Management," 1 March 2005. Document is available at : http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.

[7] CSIA, "NIAP Certification: Proposals by CSIA for Strengthening Security Certification," 23 July 2004. Organization web site at https://www.csialliance.org/home.

[8] CSIA, "Agenda for the Next Administration: Proposals by the Cyber Security Industry Alliance," 7 December 2004. Document is available at: https://www.csialliance.org/resources/pdfs/Agenda_for_Next_Administration.pdf.

program since its inception. Further, NSA has funded the development of over 70 protection profiles for use in evaluation of products for defense requirements. The continuing need for product evaluation in the defense sector is only a small portion of the NIAP need.

The principal documents concerning the NIAP for DoD are embodied in NSTISSP-11 and DoD INST 8500.1. NSTISSP-11 requires the use of evaluated products for defense and national security systems. DoD INST 8500.1 requires that product claims be based upon a protection profile, if one exists. Both of these are essential elements in the cybersecurity process. The principle document for C&A is the DITSCAP, which as of this date is not integrated with the NIAP product evaluations.

Annex D discusses the cybersecurity statues, Executive Office of the President documents, and Federal agency policies in detail. DHS, by virtue of its broader role, will be monitoring applications that are required to meet, in totality, virtually all requirements of the documents mentioned in Annex D.

3.2.2 Standards and Guidelines

For cybersecurity, the establishment of standards is critical to the ability of an organization to evaluate, acquire, and manage applications, products, or services. Congress recognized this need and designated responsibilities for development of standards and guidelines for cybersecurity for the Federal Government. In addition to standards and guidelines are best practices and protocols.

For Federal agencies, the complex mix of mandatory and voluntary standards and best practices (see Table 1) pose severe challenges in implementation for any security official. Federal agencies may have to deal with three different, and potentially inconsistent, sets of standards. Heads of these agencies have the authority to adopt more stringent standards for their entire organizations, which could mean adoption of the most stringent of the three sets of standards. Most choose not to for budgetary reasons. In the case of the NIAP and the use of evaluated products, only DoD and the NSSs must currently comply. More detail on NIST, NSSs, DoD, and Intelligence Community (IC) standards and guidelines can be found in Annex D.

Table 1. Mandatory/Voluntary Standards Matrix

Standards for Federal Systems re: cyber-security	NIST	NSA (for national security systems)	DoD	Intelligence Community	ISO/IEEE/ ANSI/ASTM	International Governmental Organizations	Regulatory Bodies (GAO, FTC, FCC, SEC, FDA, NRC etc.)
Mandatory							
Federal Government (incl contractors & grantees)	FIPS	NSTISSC/ NTSSP	DoD Issuances	DSCID 6/3, supplemented by specific IC issuances	**Deference in Lieu of Developing a Mandatory Standard**: An agency may decide that it does not need to issue a mandatory regulation because voluntary compliance with either an existing standard or one developed for the purpose will suffice for meeting the needs of the agency		Code of Federal Regulations
National (includes S/L/T & private sector)		n/a	applies to NG	tbd (IRA 2004)			Code of Federal Regulations
International (government & private sector)		CCEVS	selective applica-bility to coalition operations	n/a		NATO	collaboration w/US entities may require compliance w/CFR
Voluntary							
Federal Government	Special Pubs, Federal Agency Security Practices (BP)	security config-uration guides	STIGs (Security technical implementation guides)	n/a			n/a
National (includes S/L/T & private sector)	Special Pubs	security config-uration guides	STIGs (Security technical implementation guides)	n/a			Best practices
International (government & private sector)	Special Pubs	security config-uration guides	STIGs (Security technical implementation guides)	n/a	ISO 17799		collaboration w/U.S. entities may encourage adherence to U.S. best practices

3.2.3 Research Policy and NIAP

Because cybersecurity technology is still relatively immature, research is critical to ensuring that NIAP-relevant cybersecurity solutions are developed at the same pace as changes in IT technology. The Federal government is dependent upon the private sector for the majority of cybersecurity research, but Congress and the Executive Office of the President recognize that Federal agencies need to play an active role. The NIAP is both a recipient of the benefits of this research activity by the private sector and academia, and also an active participant, by design.

Policy makers wrongly assume that adequate research to support the NIAP needs now and in the future will be conducted.[9] Although a number of reports and documents discuss the need for cybersecurity, most are silent on the subject of research relevant to product evaluation and security evaluation metrics. In addition, any cross-pollination of research results is achieved on an ad hoc basis; no mechanisms exist to enable the identification and transition of product evaluation and security evaluation metrics research results into the NIAP community. Detailed discussion of the relevant documents can be found at Annex D.

3.2.4 Education, Training, and Awareness (ET&A) Policy and NIAP

ET&A is a critical component of any information security program, long recognized by Congress, OMB, and the Federal IT community. As with research, the NIAP is both a beneficiary of ET&A programs and a potential contributor to the increase in the body of knowledge regarding cybersecurity. A knowledgeable and competent user and practitioner community is necessary for a successful cybersecurity program. Requirements and specific assignments of responsibility for this activity are contained in numerous policy documents, described in Annex D.

NIST documents (NIST SP 800-16 and NIST SP 800-50) lay out a comprehensive ET&A program, which, if followed consistently by the Federal departments and agencies regardless of community of interest, would result in significant improvements in workforce awareness and competence in cybersecurity. As with standards, the issue is more in Federal agency consistent implementation, monitoring, and enforcement. This is a required item for reporting under FISMA 2002. OMB's FY2003 FISMA Report to Congress listed insufficient information security awareness and training as one of the

---

[9] In testimony to the U.S. House of Representatives Committee on Science in May 2003, the Defense Advanced Research Projects Agency (DARPA) Director Dr. Tony Tether described DARPA's past investments in information assurance and cybersecurity research. This work included development and improvement of firewalls, intrusion detection methods, and intrusion tolerance techniques that allow systems to operate through attacks. The bulk of this research, from DARPA's point of view, has been completed and DARPA has moved on to more advanced concepts of cognitive computing in which computer systems are expected to know what they are doing – including knowing when they are under attack and how to respond. DARPA's original firewall research has matured into widely used commercial products. The remainder of this research is still in the proof of concept and product development pipeline.

Also in 2003, the National Science Foundation (NSF) started a process to reinvigorate their Cyber Trust program. In 2004, NSF funded 50 research projects addressing different aspects of computer and network security, privacy, and trust. Virtually all of this research focuses on fundamental research questions that have long-range implications. This work, however, is not intended to address today's immediate computer security problems. Research results that can be transitioned quickly into products and applications are good, but this is not a criterion NSF uses in selecting research projects for funding.

material weaknesses in reports from 23 agencies.[10] Representative Davis's FY2004 FISMA Scorecard reiterated that "…specialized training for employees with significant security responsibilities" remains a challenge for Federal agencies.[11]

That said, there are two additional concerns about consistent implementation regarding ET&A. One is that the detailed training requirements were issued in 1998, concurrent with the establishment of the NIAP, therefore, any benefit to the NIAP process from ET&A and vice versa was not available. Additionally, the requirements have not kept pace with technology and the change in management of IT infrastructures. An update to the ET&A implementation documents issued by NIST, taking into account that both the experience from the NIAP and a reflection of maturity in Federal IT management, would be extremely valuable. The second concern is that the detail provided for functions and training requirements for both evaluators and certificate users is insufficient regarding product certification and how that is useful in system certification and accreditation.

3.2.5 Acquisition Policy and NIAP

Acquisition policy is the area that is most clearly tied to the NIAP. Cybersecurity is one of a number of factors that must be considered in Federal department and agency IT capital planning for their enterprise.[12] This approach, with significant oversight from OMB through the budgetary process, focuses on performance and outcomes from a systems perspective. To the extent that a specific IT security product performs as specified and produces desired outcomes within the enterprise infrastructure, a particular Federal department or agency will make a buy decision. If that product has been evaluated, so much the better, but that is not the primary factor, and for these agencies, there is no requirement to do so. NIST does provide guidance to Federal agencies on how to choose evaluated products.[13]

---

[10] OMB, "FY 2003 Report to Congress on Federal Government Information Security Management," 1 March 2004, p. 23. Document available at http://www.whitehouse.gov/omb/inforeg/fy03_fisma_report.pdf.

[11] Chairman, House Government Reform Committee, Representative Tom Davis, "Statement on 2004 Federal Computer Security Report Card Grades," 16 February 2005. Document available at http://reform.house.gov/GovReform/News/DocumentSingle.aspx?DocumentID=6813t.

[12] NIST provides guidance to Federal agencies through the following document: NIST SP 800-65, "Integrating IT Security into the Capital Planning and Investment Control Process," January 2005. Document available at http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf.

[13] NIST SP 800-36, "Guide to Selecting Information Technology Security Products," October 2003. Document available at http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf. NIST SP 800-23, "Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products," August 2000. Document available at http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf.

For NSSs and DoD, which are required to use evaluated products, the primary factor is whether the product has been evaluated, not necessarily that it performs the desired functions and produces the desired outcomes in the best way possible for the enterprise. It may be that the best available product has not been evaluated and the manufacturer has no intention of doing so. In that case, NSSs and DoD must rely on a lesser product whose manufacturer has been willing to go through the NIAP process. There are also situations where no product in a particular category has been evaluated.

3.3 Summary of Policy Findings and Recommendations

Reviewing the policy landscape and how policy around and about the NIAP has been implemented has identified a number of issues, which are listed in this section as Findings. Some of the issues involve the NIAP itself, most are external to the NIAP and involve agencies across the Federal Government. The Recommendation describes a desired activity to resolve the issue described in the Finding. Where possible, a specific agency with responsibility in an area of concern is identified in the Recommendation.

3.3.1 Cybersecurity

The question is whether the NIAP process should be made mandatory for than the NSSs and DoD. There is also the concern of how to integrate an evaluated product – whose configuration when evaluated may change – into the certification and accreditation process for government IT systems.

Finding [FPCy-1]

The complex policy landscape and lack of a single source for current and superseded policies makes it difficult for Federal departments and agencies to determine the requirements for their particular situations.

Recommendation [RPCy-1]

There needs to be a single source, available to all, that maintains copies of all current and superseded policy documents. This source should be available on-line, with a sophisticated search capability. A single Federal organization (such as NIST or DHS/NSCD) should be responsible for this activity and be resourced accordingly.

Finding [FPCy-2]

The NIAP was created by agreement between two agencies in different Federal departments, with no formal recognition by OMB or Congress. It has no official standing other than the agreement, which can be modified, rescinded, or terminated unilaterally by either of the two parent agencies.

Recommendation [RPCy-2]

If it is determined that the NIAP provides a valuable service, it should be formally recognized and chartered by the appropriate entity. This chartering would include specific

descriptions of the responsibilities of the two parent organizations regarding resources (funding, staffing, and facilities) and management.

Finding [FPCy-3]

The NIAP's budget is not a line item in either parent agency's budget, preventing detailed oversight of the budget process to determine sufficiency and justification. This has resulted in decreasing available resources as the parent agencies address more pressing issues.

Recommendation [RPCy-3]

The budget for the NIAP should be identified by specific line item and justified in the parent agency's (DoD/NSA and Department of Commerce/NIST) budget. This will allow for oversight to ensure sufficient funding for the NIAP's mission.

3.3.2 Standards

Finding [FPSt-1]

The National Technology Transfer and Advancement Act [NTTAA] of 1995 requires the use of voluntary consensus standards in lieu of developing Federal standards. Federal agencies' determination of which standards to use requires the mapping of existing voluntary consensus standards, Federal standards (Federal Information Processing Standards (FIPS)), and standards from the different communities of interest to determine gaps, conflicts, and overlaps. To date, this mapping has not been done, or if it has, it was not evident to the researchers in this study.

Finding [FPSt-2]

The existence of the communities of interest results in differing sets of potentially conflicting and non-interoperable requirements. Although FIPS issued by NIST are mandatory for the Federal Government, national security systems (NSS) are exempt from them. NSSs have their own standards and guidelines as do DoD and the IC. Annex D provides more detail on the standards for these communities of interest.

Although Federal departments and agencies are at liberty to establish a single set of requirements for their activities based on the most stringent requirements, it may not be feasible for all to do so. The Computer Security Act (CSA) of 1987, Clinger-Cohen Act (CCA) of 1996, and Federal Information Security Act (FISMA) of 2002 encourage NIST to work with DoD and NSA to synchronize standards; the ability to achieve much in this area depends upon emphasis and resources.

Recommendation [RPSt-1]

NIST should work with NSA, DoD, and the IC to synchronize existing and future standards to reduce the potential of conflicting and non-interoperable requirements among the communities. Although NIST development is open and input is solicited from all entities, a more proactive formation of consortiums and alliances is suggested.

3.3.3 Research

Finding [FPRe-1]

Current levels of cybersecurity research funding are inadequate and fail to address current cybersecurity issues, much less those of the future (such as grid computing, distributed intelligent agent systems, distributed knowledge management, composable systems, and systems of systems) (See Footnote 9).

Finding [FPRe-2]

A timeline, schedule, and process for addressing future cybersecurity concerns are lacking.

Finding [FPRe-3]

A process for coordinating government efforts and allocating research resources for cybersecurity research is lacking.

Recommendations [RPRe-1]

DoD and NIST should develop a strategic plan for investigation of future NIAP-related cybersecurity needs and conduct the research required to address the needs. White House Office of Science and Technology Policy (OSTP) should set national cybersecurity research priorities and the research agenda and coordinate research efforts among government organizations. OSTP should develop a mechanism for coordination of government cybersecurity research efforts.

Finding [FPRe-4]

The memorandum establishing the NIAP says that NIAP seeks to foster research and development in security tests, methods, and metrics, but to date this has not happened.

Finding [FPRe-5]

The memorandum establishing the NIAP says that NIAP seeks to foster research and development in security tests, methods, and metrics; however, there is no plan or process in place to identify the necessary research or to ensure that the research is performed.

Recommendation [RPRe-2]

NIAP should develop a plan and undertake the research required to foster research and development in security tests, methods, and metrics.

Finding [FPRe-6]

While some portion of information security research advances achieved as a result of the Homeland Security Act of 2002 may be of use for the NIAP, no process is in place to identify those results or to transfer them into the CCEVS process.

Finding [FPRe-7]

The need for research to improve the quality of our cyber defense and defensive information operations is widely acknowledged in numerous government documents;

however, no document points to the NIAP as a tool for addressing this need or directs research that would result in the NIAP being able to address this need. In the few cases where the need for research is identified in a document, it is usually cited in relation to a specific threat, such as mobile malicious code, and never addressed toward improving the capability to determine whether software is secure via the NIAP process.[14]

Finding [FPRe-8]

While the Clinger-Cohen Act imposes a research duty upon the National Science Foundation (NSF), there is no mechanism for communicating the NIAP's needs to the NSF or for extracting NSF research advances and employing them for NIAP purposes.

Recommendation [RPRe-3]

The NIAP should develop, under OSTP guidance, a process to identify and transition successful NIAP-related research to the NIAP laboratories, developers, and evaluators. OSTP should develop a process to ensure successful transition of cybersecurity research results across government organizations.

3.3.4 Education, Training, and Awareness

Finding [FPEta-1]

The training documentation produced by the NIST for the Federal Government (SP800-16) in 1998 was issued concurrently with the establishment of the NIAP. Although a model program when it was issued, the changes in policy, technology, management of Federal IT organizations, and organization require a similar significant update to this document.

Finding [FPEta-2]

The level of detail in the current NIST SP800-16 is insufficient to ensure an appropriate level of knowledge for either the NIAP certificate users or certifiers (see also 5.3.1, 5.3.2, and 5.3.4). This increased level of detail is necessary for evaluation of the performance of those functions.

Recommendation [RPEta-1]

NIST ET&A documents (not all of which have been mentioned) need to be updated to address changes in policy, technology, management, and organization of Federal IT. Additionally, sufficient detail should be included to address the deficiencies noted for the NIAP certificate users and certifiers (see also 5.3.1, 5.3.2, and 5.3.4).

[14] For the purposes of this report, research into proof of correctness of software is not considered to be equivalent to research into proof of security capabilities and quality of software.

3.3.5 Acquisition

Finding [FPAq-1]

Although FISMA documents specify the security controls that must be implemented in Federal unclassified systems, there is no requirement for how Federal agencies must choose those products. The requirement for acquisition of evaluated IA/IA-related products only exists for the NSS and DoD. Outside of this, no acquisition policy concerning IA/IA-related products has existed for Federal departments and agencies since the Federal Information Resources Management Regulations (FIRMR) was rescinded in 1996. This means that the rest of the Federal Government can choose security products based on their own criteria that may or may not have been evaluated.

Recommendation [RPAq-1]

Consideration should be given to making an improved NIAP product evaluation process[15] mandatory for all Federal Government entities. This must be conditioned upon several actions that improve the usefulness of the product and, where possible, reduce overall costs. The resources necessary to accomplish this must also be available.

Recommendation [RPAq-2]

An official statement of policy from the appropriate entity should be made that the NIAP is the U.S. Common Criteria Evaluation and Validation Scheme for achieving the requirement for DoD to use evaluated products. Under mutual recognition, the DoD could use products evaluated under other national schemes as well. This should be done only after improvements are made under Options 4 and 5 of Chapter 8.

Finding [FPAq-2]

The NIAP process leading to product certification does not directly contribute to the systems certification required by statute and OMB.

Recommendation [RPAq-3]

NIST and NSA should make the relationship explicit between the NIAP process and the process for C&A of systems. This includes descriptions of how to use the products from the NIAP process to feed into the C&A process. This is a requirement for the recommendations above.

[15] Improved as outlined in either Option 4 or 5 of Chapter 8. These improvements should result in effective and integrated product evaluations.

4. NIAP and Evolution

This chapter describes the NIAP and how it has evolved from its inception to its current organization, responsibilities, and operations. This is the second in a set of three independent analyses of the cybersecurity landscape and the NIAP as it fits into that landscape. The timeline of activities that led up to the formation of the NIAP and the flurry of activities that followed are included in Annex E. The timeline at the end of Annex E shows that the development of this partnership and the approach to product evaluation was not a spur-of-the-moment undertaking. The NIAP is an outgrowth of the many initiatives in cybersecurity by both NIST and NSA and in response to the policy landscape described in the previous chapter. It was well thought out by a number of professionals and intended to provide a viable product evaluation scheme as a part of an overall cybersecurity program.

4.1 The NIAP's Original Charter

As described in Chapter 1, the NIAP is a joint effort between NIST and NSA to provide technical leadership in the research and development of security-related IT test methods and assurance techniques. The Terms of Reference document that established their collaboration [NIST/NSA1998] set forth the following goals for the NIAP:

- Promote the development and use of evaluated IT products and systems;
- Champion the development and use of national and international standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the U.S.

The most significant component of NIST and NSA's collaboration is the Common Criteria Evaluation and Validation Scheme (CCEVS). CCEVS is the NIAP's product evaluation process, which has evolved from NSA's earlier Trusted Product Evaluation Program (TPEP). As the "CC" in its name implies, CCEVS is based on the International Common Criteria for Information Technology Security Evaluation [ISO International Standard 15408]. CCEVS supports many of the goals outlined above.

NIST and NSA separately fund (or do not fund) their respective contributions to the NIAP. NIST contributions have been minimal. The two agencies have separate responsibilities for IT security under the Computer Security Act of 1987 and later legislation. The NIAP activities, therefore, reflect each agency's priorities. Both agencies agreed that evaluations were the highest priority and the result is the CCEVS. Beyond this, NIST conducts laboratory accreditations and has developed training materials, primarily for prospective evaluators. NSA has developed evaluation training, and a number of Protection Profiles (PP), which provide standard evaluation criteria for products of a particular type, such as firewalls. These PPs are intended primarily for DoD use. NSA has played an important role in interpreting the letter and intent of the Common Criteria (CC) when questions have been raised during evaluations. They have also been heavily involved in the development and evolution of the CC.

Areas identified in NIAP's goals that have not received the same level of attention as the CCEVS include IT security research, development of tools for security testing, and metrics for assurance.

4.2 CCEVS for IT Security

A formally established group called the CCEVS Validation Body is responsible for the operation of the validation scheme. The Validation Body's principal objective is to ensure the provision of IT security evaluation and validation services for both government and industry.[16] This group was formally established in response to the Common Criteria Recognition Agreement (CCRA).

The NIAP established the following objectives in developing, operating, and maintaining the evaluation and validation scheme[17]:

- Meet the needs of government and industry for cost-effective evaluation of IT products;
- Encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- Ensure that security evaluations of IT products are performed to consistent standards; and
- Improve the availability of evaluated IT products.

The validation scheme is intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, IT product consumers, auditors, and accreditors

[16] http://niap.nist.gov/cc-scheme/.
[17] http://niap.nist.gov/cc-scheme/ccevs-objectives.html.

(individuals deciding the fitness for operation of those products within their respective organizations). Close cooperation between government and industry is paramount to the success of the scheme and the realization of its objectives.

Commercial testing laboratories called Common Criteria Testing Laboratories (CCTL) carry out the NIAP product evaluations. These laboratories are accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body. NVLAP accreditation is one of the requirements for becoming a CCTL. The purpose of NVLAP accreditation is to ensure that laboratories meet the requirements of ISO/IEC 17025:2005, General Requirement for the Competence of Calibration and Testing Laboratories [ISO2005] and the specific scheme requirements for IT security evaluation.

During the course of an evaluation, the CCEVS Validation Body provides technical guidance to those testing laboratories, validates the results of IT security evaluations for conformance to the CC, and serves as an interface to other nations for the recognition of such evaluations.

Upon completion of a successful evaluation, the CCEVS Validation Body issues the evaluated product or protection profile a CC Certificate. This certificate confirms that the evaluation was conducted by an accredited laboratory using the Common Evaluation Methodology (CEM), and that the conclusions of the testing laboratory are consistent with the evidence presented during the evaluation.

All IT products and protection profiles that have successfully completed evaluation and validation appear on the Common Criteria Validated Products List (VPL). This list includes those products and profiles successfully completing similar processes under the schemes of authorized signatories to the Arrangement on the Mutual Recognition of CC Certificates in the Field of Information Technology Security. The U.S. CCEVS has currently been limited to products that claim some information assurance (IA) properties. This is mandated in NTSSISP-11 for defense critical and intelligence IT system applications, and is true of those on the lists. This has not been applied to the wide range of products that may reside in an IT system and affect its security.

4.2.1 Evaluation Process

The NIAP product evaluations follow a well-established process that involves at least four sets of participants. The players are:

1. The sponsor, who is often the product developer or their agent;
2. An evaluation laboratory;
3. The CCEVS Validation Body; and
4. An evaluation validator assigned by the CCEVS Validation Body.

The steps in the process are shown in Figure 5. The starting point is when the sponsor determines the need for an evaluation. The sponsor must decide whether the product is to be evaluated against an existing protection profile (PP[18]) or against a unique set of claims. These claims have to be documented in what the CC call a security target (ST). An ST is required for every evaluation. Claims of conformance to PPs are not partial and any claim means that all of the provisions of the PP are covered in the ST. If any provision of the PP is removed from the ST, the claim to conformance to the PP must be dropped. PPs have predetermined evaluation assurance levels (EAL). If a PP is not used, the EAL (or a set of assurance requirements) for the evaluation must also be decided. While the CC make no requirement on the choice of assurance requirements, an EAL package is generally selected (exceptions do exist).

Figure 5 shows the process for evaluations at EAL4 and below. Evaluations above EAL4 follow a similar process with a fifth participant, NSA, taking responsibility for additional testing and vulnerability analysis. The additional testing and analysis is done after the lab has completed their testing and submitted their Evaluation Test Report (ETR).

The next step in the process is for the sponsor to contract with a lab to conduct the evaluation. The lab then puts together an evaluation proposal package consisting of the sponsor's product description and security target, and their work plan and schedule. This proposal package is then submitted to the CCEVS Validation Body for approval. If the CCEVS finds discrepancies in the proposal, they return comments to the lab and sponsor for resolution.

Once the CCEVS Validation Body accepts the proposed evaluation, they assign a validator to monitor the evaluation as it progresses. The validator works with the lab throughout the evaluation to ensure that it is conducted as planned and meets all CC requirements. When the validator is satisfied with all the details in the lab's work plan, they hold a kickoff meeting to formally start the evaluation. At this time, the product is entered on the CCEVS official list of products in evaluation.

[18] The protection profile is a set of requirements, both functional and assurance, for a class of products (such as a firewall). It may specify precisely, or allow certain latitude in achieving, these functionalities. It is normally developed by a set of domain experts in a community of interest. NSA has developed a number of PPs for DoD use.

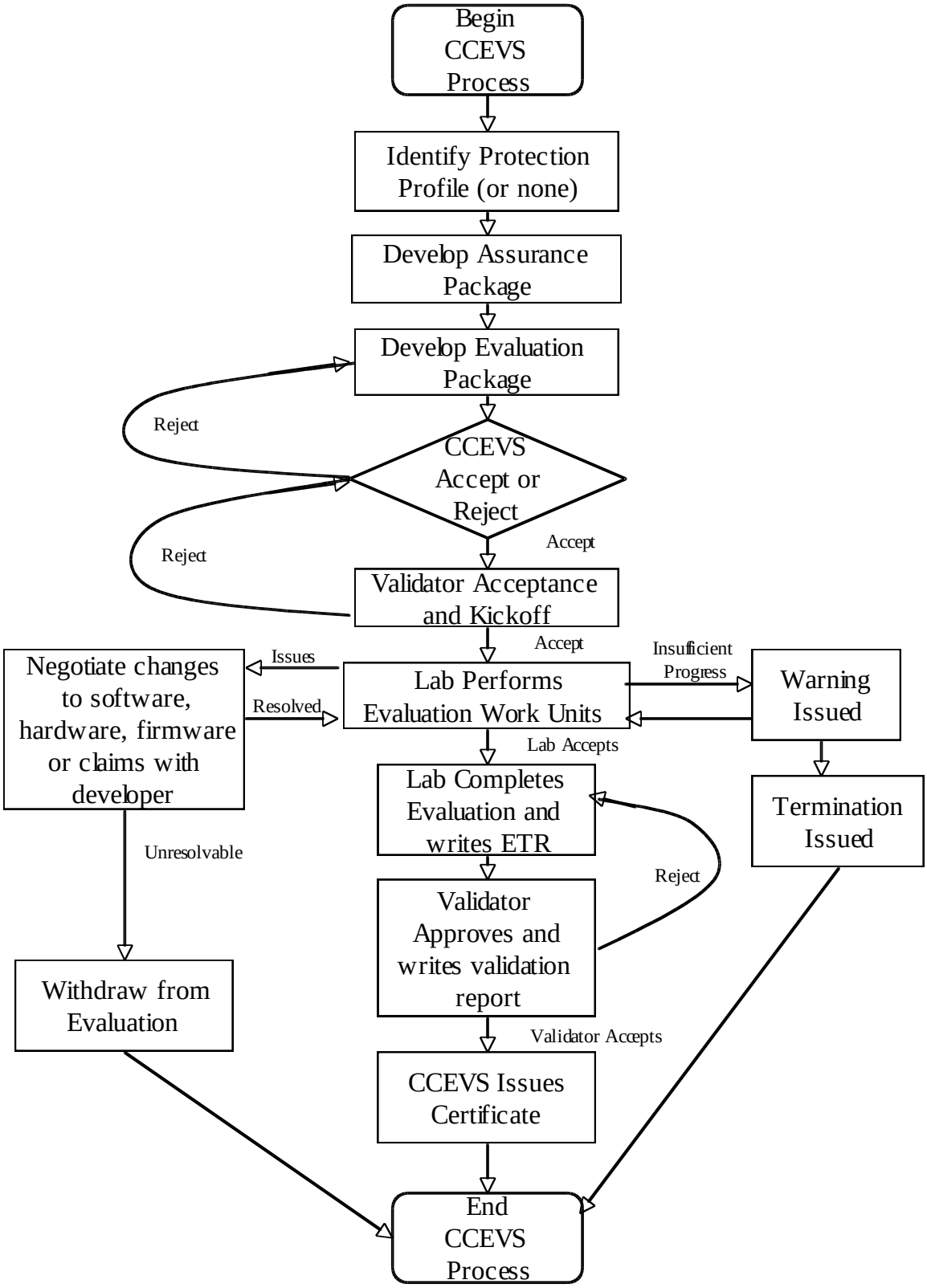


Figure 5. Overview of the NIAP Evaluation Process

In conducting the evaluation, the lab typically starts several parallel activities to review product documentation and prepare for testing. For example, the security target claims are reviewed and a test plan is developed. The test plan covers the requirements of the EAL as delineated in the Common Evaluation Methodology (CEM). Below EAL4, testing is minimal and survey in nature. Other documentation includes the product's configuration management record, description of the product's design, user manuals, and product delivery procedures. Documentation may include the low-level and high-level design documents, correspondence documents, and security interface specifications and summary specifications. No specific format is required by the standard, only content. However, in practice, separately prepared documents are generated in lieu of usage of the developmental documentation. Preparation of these documents and the preparation and revision of the ST may be undertaken by the developer or by a consultant hired by the developer. In many instances, the developer will contract with a separate group at the evaluation lab for the preparation of evidence, which is allowed under CCEVS rules, as long as separation between evaluation and evidence preparation is demonstrated. Any discrepancies the lab finds are brought to the sponsor and developers' attention for resolution.

The validator monitors the lab's activities throughout the evaluation. This monitoring includes review of ETR sections for compliance with CC and CCEVS, witnessing tests, and other oversight activities. At the conclusion of the evaluation process, the validator must accept the lab's ETR. To ensure the evaluation remains on track, several milestones are typically observed. For example, the lab will have the validator approve their test plan before proceeding to conduct the tests. During testing, the lab will have the validator check their procedures and validate the results they are collecting. Keeping the validator in the loop minimizes the possibilities of surprises later in the process.

If testing reveals discrepancies – that is, if the product fails to meet an ST claim – the sponsor and developer are engaged to resolve the problem. If the product's problems cannot be corrected, the claims it is unable to meet must be removed from the ST. Any changes to the ST are first reviewed and commented on by the validator. The validator can also raise significant ST issues with the CCEVS Validation Body to keep them aware of lowered product expectations. The CCEVS Validation Body might want to know, for example, that a product that was being evaluated against a PP is not able to meet all of its requirements. This may result in dropping a claim to PP performance or changes to the software, hardware, or firmware as needed to meet PP conformance. In the latter case, delays in the evaluation may occur.

Vulnerability analysis is usually the final stage of the evaluation process. Checking for vulnerabilities begins at EAL2, but serious vulnerability testing (AVA_VLA.3) is ordinarily not required until above EAL4. As with other testing, any vulnerability

discrepancies that are found are raised with the sponsor and developer for resolution. Occasionally, analysis may discover very obscure vulnerabilities that have little chance of being exploited. If the developer is unable to correct the problem, the product may still complete and pass its evaluation by modifying the ST as to threat or objectives. The validator, in this case, may question whether the vulnerability is applicable for systems built from components at this evaluation's assurance level. This ruling may be appealed to CCEVS.

Alternatively, the threat environment in the ST may be modified so that no claims to counter that particular vulnerability are made. If a PP is claimed for conformance, the ST cannot lower the threat expectation and still claim PP conformance. DoD requires the ST to be based upon an NSA-approved PP. At the conclusion of documentation reviews, the lab will finalize its Evaluation Technical Report and submit it, along with the ETR, to the CCEVS Director. When the Director, in conjunction with the CCEVS Chief Validation Body, accepts the findings of the evaluation and the validation report, a certificate is issued for the product and the product is placed on the VPL. Two lists were mentioned, and both are significant to DoD. The first is the list of products in evaluation, and the second is the VPL. NSTISSP-11 requires a product to be on one of these two lists for use in defense or national security systems.

Sources used in this analysis included the Common Criteria [CC2004a, b, c], CCEVS evaluation process descriptions [CCEVS11999], [CCEVS22000], [CCEVS32002], CCEVS42001], and [CCEVS52000], and informal interviews with NIAP personnel.

4.2.2 Built-In Assumptions and Associated Risks

Our analysis of the current NIAP evaluation scheme uncovered a number of assumptions that appear to have driven the formulation of these processes. Many of these assumptions were recognized in developing the CCEVS, and checks and balances were included in the scheme to ensure that potential problems would be contained. Other assumptions appear to be implicit, as evidenced by how evaluations are conducted under the CCEVS. These assumptions have fewer safeguards and represent larger risks. Both sets of assumptions were derived from CCEVS documentation, observation, and personal experience of analysts on the evaluation team.

4.2.2.1 Evaluated Products Assumptions

The first set of assumptions concerns the products that have been through evaluations and how and where they are used.

The next group of assumptions concerns the methods and techniques used in evaluations, and results from evaluations.

Component Security [AN-01]

Evaluated components are assumed to provide better security for the systems of which they are a part. It is further assumed that system integrators will build systems intelligently using appropriate components. (These are key assumptions. If there are exceptions, evaluated products may not live up to expectations.)

Dubious Evaluations [AN-02]

The CC allows evaluations of products that provide little or no protection. Examples include partial product evaluations, trivial security requirements, and evaluations of simple electrical components. The CCEVS provides no safeguards against such evaluation abuses. Certificates must be issued for products that pass these evaluations, even though they provide little if any useful protection. However, Validation Reports should articulate shortfalls and differences between the portions of the product that were evaluated and the product as used in a typical configuration. It should be noted that the user decides usefulness, and the concern becomes significantly less when Education, Training, and Awareness have provided most users with the information to read and interpret an ST. Such education would allow the user to better evaluate the ST claims.

Evaluation Processes and Results Assumptions

The next group of assumptions concerns the methods and techniques used in evaluations, and the results from evaluations.

Comparability and Consistency [AN-03]

Evaluations based on the CC are assumed to be comparable and consistent. Validation is tasked with providing that level of consistency. That is, if different labs were to evaluate the same product, they would produce virtually identical results. Evaluations performed in other countries under Mutual Recognition Agreements (MRA) are assumed to be conducted with the same quality and consistency as under the NIAP's CCEVS.

Single Evaluation [AN-04]

The CC assumes a security evaluation needs to be performed only once, worldwide, for a given version of a product in a given type of environment. The risk here is that information systems and environments are constantly changing, often without full consideration of security impacts. The Maintenance Assurance packages do make provisions for continued and partial re-evaluations, but these are not part of any assurance-level packages. Several DoD protection profiles do invoke these assurance requirements.

Point Evaluations [AN-05]

Each evaluation will consider only one specific version of a product, for a specific environment. Even if there is no assurance maintenance or flaw remediation process for the product, the results of evaluations are assumed to be useful to consumers for the foreseeable future. This last point is a conjecture.

Few Protection Profiles [AN-06]

PPs were intended to provide standard sets of claims against which products that perform similar security functions would be evaluated. It was assumed that PPs would be developed covering a wide range of security needs and that these PPs would serve as standards for product comparisons. NSA has created some 70 PPs to address military security needs, but very few have been developed or adopted for commercial and civilian government use. These PPs have not been extensively vetted through consumer and private organizations, and are generally not thought of as available for general use. Few product evaluations (other than DoD applications) make PP claims, leaving consumers with little basis for comparing competing products. Unless a product is meant to satisfy an identified military need, the product vendor is left to decide the security claims the product is evaluated against. While the development of PPs to cover all contingencies should not be part of the NIAP's requirements, the fostering and support of industry consortiums to do this should be.

Vulnerability Testing [AN-07]

CC evaluations are assumed to include sufficient analysis and testing to detect obvious security vulnerabilities. The CC, however, defines only a general process for describing attack (e.g., level of effort and knowledge required). The CEM also provides only general guidance on various types of attacks to consider.

The NIAP requires no specific vulnerability testing for even commonly evaluated products (such as firewalls, Portable Operating System Interface (POSIX) operating systems, or IDS systems). No standard test suite has been developed for vulnerability testing. There is no requirement to use automated vulnerability analysis tools (such as source code scanning tools or input injection tools) to perform vulnerability analyses.

Source Code Review [AN-08]

Evaluators are assumed to have access to all product information necessary to assess the product's security properties. The CC do not require evaluators to perform independent reviews of product source code for security purposes. For software products the source code is ground truth, containing essentially everything evaluators need to know about its behavior. Source code, however, is not available for EAL3 and below. Only at EAL4 and higher is a complete set of source code made available. Manual

reviews of source code can be expensive or impossible for large software systems. Automated tools can be used to identify critical code components and focus reviews. While use of such tools is permitted, it is not required at any EAL. This is both a NIAP responsibility and a CC responsibility.

Coding Errors [AN-09]

The evaluation process assumes that developers generally know how to implement secure software; that is, coding errors that result in security problems are rare and unlikely. Otherwise, code-checking tools would be applied to the software. Evaluations concentrate on the requirements and design documentation instead of the implementation. Most security vulnerabilities, however, can be traced to common implementation errors. Unfortunately, relatively few developers know how to avoid security flaws because this is not taught at most universities. Annex F includes references justifying the claim that most vulnerabilities are caused by common implementation errors. The annex also shows that tools can detect many of these vulnerabilities, but as noted above, such tools are not required by the CC.

Requirements Tracing [AN-10]

Documentation that traces requirements through design and implementation (depending on the EAL) is assumed to be an effective security analysis technique. These so-called representation correspondence requirements, especially at the upper EAL, impose traceability requirements far in excess of typical commercial development practice. As a result, the developer must spend significant effort writing or re-writing documentation; in many cases long after product development has been completed. This documentation effort rarely contributes to finding security flaws.

Documentation Requirements [AN-11]

CC product documented information requirements are fixed and highly inflexible. They assume that all development methodologies produce the same detailed documented information and that resulting products are susceptible to the same security flaws. Commercial software development practices, however, differ widely and rarely produce the classical “waterfall model” documentation expected by the CC. While attention to well-established software development and documentation practices generally corresponds with better product quality and product documentation, product security requires a particular focus that is not assured by the CC’s documentation requirements. The current requirements lead CC evaluations closer to evaluating the quality of documentation instead of the quality of the product.

Documentation after the Fact [AN-12]

Product design documentation provided as evidence in evaluations is assumed to represent the design the product was actually based upon. Developers, however, can provide evaluators' design documentation prepared after the product has been completed, which does not necessarily reflect how the product was developed. A third party who may or may not understand how the software was developed may actually produce this documentation. In general, documentation produced late would be acceptable if it were accurate.

Evidence Availability [AN-13]

Public evaluation results are assumed to provide sufficient information about test results and evidence collected in evaluations for consumers to make informed decisions about products. Details of test results and other evaluation evidence contained in Evaluation Technical Reports (ETR), however, are not included in certificates and are not available for public review. There is a need to make these reports more easily understandable. Proprietary interests in the ETR and test result documents need to be resolved.

For information about tools to support evaluations (e.g., for proactive measures, vulnerability testing, source code reviews), see Annex F.

4.2.2.3 Assumptions about Product Users

These assumptions concern IT system users, customers, consumers, and owners.

4.2.2.3.1 Use of Evaluated Products [AN-14]

To comply with national and agency information assurance policies, information system owners must buy products that have been evaluated, and they may assume this means that evaluated products meet their (or someone's interpretation of their) security needs. This may be partially true with conformance to a properly vetted PP. Chapter 5 reviews the expectations in this area. While no one has provided this assurance, it is nonetheless a problem.

4.2.2.3.2 Diverse Security Requirements and Assurance Needs [AN-15]

Not all information systems have the same security policies and requirements. Not all information system owners need the same level of assurance in the security of their systems. Evaluated products are assumed to support construction of systems with different security requirements and different levels of assurance. The ultimate responsibility for use of the product is with the system developer. He should be given broad access to evaluation documentation.

4.2.2.3.3 Paying for Evaluations [AN-16]

Security is assumed to be important enough to information system owners (including the U.S. Government) that either they will pay enough extra for evaluated products to make evaluations economically viable for the vendor or they will pay for evaluations themselves.

4.2.2.3.4 Smart Consumers [AN-17]

IT system users and administrators are assumed to always read and follow all security-related guidance (including installation guidance) provided to them; this is a dubious assumption. Careful attention should be paid to default configurations. Consumers are assumed to know their security requirements and purchase only those evaluated products that meet their needs. This further assumes that consumers will use an evaluated product only in the environment in which it was evaluated, or that the ST and public evaluation material provide enough information for them to understand how the product will perform in their environment.

4.2.2.4 Assumptions about Product Developers

These assumptions concern the behavior of product developers.

4.2.2.4.1 Full Disclosure [AN-18]

Developers are assumed to disclose all information relevant to product evaluations, such as design documentation and results from their own testing, and not hide knowledge of vulnerabilities, back doors, or other flaws from evaluators. Because of the distributed nature of many software development projects, the developer may not even know these things himself. However, this assumption is less of a problem if the education, training, and awareness of developers is at a high enough level that they can precisely articulate what they know and don't know about their products.

4.2.2.4.2 Trustworthy Developers [AN-19]

Product developers are assumed to be trustworthy and not knowingly insert malicious code into their products. Because of the distributed nature of many software development projects, the developer may not even know these things himself.

4.2.2.4.3 Impact of Evaluation Costs [AN-20]

The cost of evaluations is assumed to be insignificant (or at least not prohibitive), so small businesses and independent developers, as well as large corporations, can have products evaluated. The typical cost of $100,000 or more for an evaluation (with additional costs to the internal processes of the vendor), however, is a barrier to entry for open source software (OSS) and many products developed by small businesses.

4.2.2.5 Assumptions about Evaluation Laboratories

The final set of assumptions concerns the evaluation labs.

4.2.2.5.1 Evaluation Independence [AN-21]

A product's security evaluation is assumed to be an unbiased assessment, not influenced by the developer or vendors with financial interests in the product. This is also a requirement of NIST Handbook 150-20.

4.2.2.5.2 Laboratory Competence [AN-22]

Labs that are approved to perform evaluations are assumed to have demonstrated their competence in conducting evaluations and maintain that competence. In addition to the laboratory's general level of competence, each evaluation team within that lab is assumed to be competent. This is also a requirement of NIST Handbook 150-20.

4.2.2.5.3 Commercial Viability [AN-23]

The demand for evaluations is assumed to be high enough to make commercial product evaluation labs viable.

4.2.2.5.4 Laboratory Competition [AN-24]

Competition among evaluation labs is assumed to be sufficient to keep evaluation costs to a minimum, without losing quality. This is also a requirement of Handbook 150-20.

4.2.2.5.5 Flexibility [AN-25]

Evaluation labs are assumed to be flexible in their ability to accommodate shifts in the number of products, new and different types of products, and changes in security technology.

4.2.2.5.6 Proprietary Evaluation Processes [AN-26]

Detailed processes used by labs to perform evaluations (beyond what is in the Common Evaluation Method) are proprietary and may be hidden from the public and other labs.

4.2.2.6 Assumptions about Policies Concerning Evaluations

This group of assumptions addresses national and agency policies relating to evaluations.

4.2.2.7 Only IA-Enabled Products [AN-27]

National policies identify only IA and IA-enabled products as subjects for evaluation. This assumes many products not normally considered to be IA or IA-enabled, such as web browsers, image viewers, and word processors, which are directly connected to networks, have no vulnerabilities or security impacts. Many of these products have provided unintended system access to attackers.

4.3 The NIAP Responsibilities beyond CCEVS

The NIAP's charter includes several tasks beyond setting up and operating the evaluation and validation scheme. There are two broad areas of additional responsibilities: research and development, and education and training. The first is an explicit requirement of the NIAP letter of partnership. The second is a derived requirement as part of an overall program of security product evaluations.

4.3.1 Research and Development

Three areas of research and development were identified as goals of the original NIAP charter: techniques for security requirements definition; testing methods, tools, and techniques; and assurance metrics.

4.3.2 Security Requirements Definition

Current methods for specifying information security requirements, in terms of the sensitivity of information, confidentiality, access controls and other protection mechanisms, availability, integrity, and fallback and recovery mechanisms, are incomplete and, because no standards exist, are often inconsistent. While several attempts have been made to develop taxonomies of security requirements (outside the NIAP), this remains an open research problem. Fostering and promoting consortium development of PPs is needed.

4.3.2.1 Testing Methods, Tools, and Techniques

The NIAP has sponsored projects such as the Common Criteria Toolbox. This tool is for evaluation development, however, not for improving IA code development or testing. Budget priorities have excluded development of tools that would contribute to production of more secure products.

4.3.2.2 Metrics

Little research has been funded into metrics for information assurance, the efficacy of IA methods and techniques, or the return on investments made to improve IT system security. For example, a primary metric for all evaluations would be the value of the information protected or the losses that may occur with security breaches. Neither of these is generated and tracked. Also, the cost of product evaluation is treated as

laboratory-proprietary and the data is not collected. Some data is being collected on product improvement due to evaluation, but is insufficient at this point.

4.3.3 Education and Training

Education and training is a derived requirement as part of an overall program of security product evaluations. The NIAP has developed training materials for evaluators and standards for product documentation. A major area of information assurance education and training that has not been adequately addressed is the education and training of IT system purchasers, operators, and users. The assumption of knowledgeable consumers described earlier (Sec. 4.2.1.2) is not supported in practice.

4.4 Growth of Evaluation Business

Figure 6 shows the growth in the number of evaluations that have been completed and that were in process under NIAP's supervision over the past four years. The certificates-issued-to-date data are cumulative, to date. The in-evaluation data are a snapshot for the year and may represent some products that carry over from year to year, and some products that have not and may never receive a certificate of completion. These statistics while less than ideal do serve to show a growth rate in the obligation of the "oversight" provisions that are required by the CC. The growth rate is close to 100 percent – doubling every year – and shows no signs of leveling off.

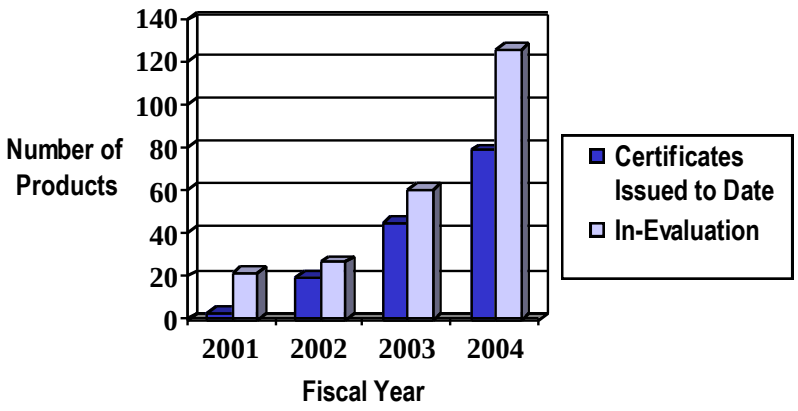


Figure 6. Growth in the Number of Evaluations Conducted Under the NIAP

The original evaluation labs have expanded their business to match this growth. There are now eight certified labs performing evaluations. The difficulties of staffing this rate of business growth with qualified personnel have been raised as an issue.[19] An even

[19] cf. Sec. 5.3.4, Evaluation Personnel and Lab Expectations and Observations.

bigger problem has been the government's difficulty in staffing validators to monitor the progress of each evaluation. Originally, going as far back as the TPEP program in the 1980s, validators were drawn from government staff and from independent Federally Funded Research and Development Centers (FFRDC). These sources have not been able to keep up with the increased demand. Several structural changes have kept the backlog to a minimum, and the NIAP is working diligently to keep up with the growth.

The rapid growth in evaluations has also drawn attention and resources away from the NIAP's other responsibilities for research and development, protection profiles, and education and training. The NIAP's funding has not increased to cover the additional obligations imposed by evaluation growth. Research into information assurance metrics, for example, has not provided a metric and tracking system. NIST started work on testing and analysis tools, but has discontinued it. NSA has developed PPs for military needs, but nobody has stepped forward to produce PPs for broader government and commercial environments. NSA developed training materials on the CC. NIST developed training materials for evaluators and validators, but information assurance education and training for the broader community of IT system owners and users has not been addressed. This was not an original requirement of the partnership, but it is needed for the consumer side of product evaluation.

4.5 Findings and Conclusions

4.5.1 Finding [FN-1]

NSA and NIST, without separate funding earmarked for the NIAP, have produced a flexible, capably staffed, although under-funded product evaluation system.

4.5.2 Finding [FN-2]

Budgeting restrictions have prevented the NIAP from developing education and training resources for IT system consumers, tools to support secure product development, and protection profiles for non-military applications.

4.5.3 Finding [FN-3]

Oversight of evaluations has been limited due to stretched NIAP budgets and a shortage of qualified validators. The oversight mechanism meant to ensure that evaluations conform uniformly to all CC requirements is under-funded. The NIAP has made adjustments in both organization and resources. The current number of evaluations stresses the limits of the validation resources, and the number of evaluations continues to grow.

4.5.4 Recommendation [RN-1]

Addressing the NIAP's shortcomings requires giving the NIAP a more substantial footing organizationally and sufficient, stable funding to achieve its tasks. Although there is some need for evaluation scheme improvements (see Chapter 5 on stakeholder expectations), there is no need to start the process over from scratch. Revamping the administrative structure processes and developing the expertise needed to create an alternate product evaluation scheme would be costly and time consuming, and there is little evidence that a more successful result would be achieved.

4.5.5 Finding [FN-4]

Evaluations take longer than anticipated. Evaluation schedules are often extended beyond what was originally planned.

4.5.6 Finding [FN-5]

Evaluations frequently result in modified products or claims. Most evaluations take longer than anticipated either because the product does not satisfy the initial claims or because the documentation is not adequate. The result is that either the product or the claims must be modified. This is actually a good thing if one ascribes to the "truth in advertising" approach, and reduction of claims in marketing materials would follow. However, sufficient data gathering has not been done to adequately quantify this effect. It appears (from experienced evaluators and validators) that the evaluation documents are the primary place that claims are reduced. Ideally, the product would be modified to meet the claims, but it is usually easier to obtain a certificate by reducing claims. The NIAP is working to have claim adjustments documented, but this only helps sophisticated customers who read the documentation. When conformance to a PP is cited or required, the claims in the ST cannot be reduced below those of the PP. DoD requirements for PP conformance should be continued.

4.5.7 Finding [FN-6]

Developers produce large amounts of data relevant to evaluations during their development and testing. Only a small portion of this data is provided to evaluators in the form of evidence. Consumers typically see only the product's evaluation certificate, which contains no vulnerability information, and the other information available to them is written in precise evaluation language and typically has little information about residual vulnerabilities. Education, Training, and Awareness (ETA) have lagged, so consumers are generally not well educated in reading the evaluation reports.

4.5.8 Recommendation [RN-2]

Vulnerability analysis and testing results from product evaluations should be made available for system-level C&A. This availability can be through the laboratories or the development of sanitized reporting methods.

5. Perceptions of Issues, Problems, and Expectations

This is the third in a set of three independent analyses of the cybersecurity landscape and the NIAP as it fits into that landscape. This part of the study solicited perceptions about NIAP issues, problems, and expectations from cybersecurity stakeholders. It is important to understand what stakeholders believed the NIAP was doing and how well, and compare those beliefs to The NIAP's objectives and observable performance. Perception, by definition, is tricky because no two people see a problem in exactly the same way. To balance individual perceptions and shed light on problems perceived by different parts of the information technology community, stakeholders were grouped into classes. The categories set up were intended to cover the entire community. The sample is not statistically significant (not a distribution-based sampling), but it is representative of the community as a whole and was used to raise issues.

The principal data collection tool was the personal interview, although additional data were gleaned from written material, personal communications, and team member experiences. On October 22, 2004, IDA hosted a forum to solicit broader input. At this forum, individuals representing all stakeholder classes were invited to participate in a review of the data gathered to date and provide input on additional issues, problems, and expectations. Finally, a notice soliciting additional input was placed in the *Federal Register*. This chapter synthesizes the inputs from all of these sources.

The first section of this chapter describes our data collection processes. The second section describes the analysis process used to synthesize the results. This led to the identification of 16 different topic areas that were of concern to stakeholders. The third section presents the expectations, observations, and findings derived for each of these topic areas.

5.1 Data Collection Processes

This section describes our interview process, as well as the other mechanisms used for data collection.

5.1.1 Stakeholder Classes

To ensure thorough data collection coverage of an expected wide range of perceptions about the NIAP, the analysis team divided the population of IA stakeholders into the following categories:

1. **Department of Defense (DoD) –** Individuals in the DoD who represent the assured information system customer base;

2. **Federal Government (FEDNonDoD) –** Individuals outside of the DoD but in the Federal Government who represent the customer base (such as the National Aeronautics and Space Administration (NASA) or the Federal Aviation Administration (FAA));
3. **Process –** Individuals who are or have been involved in executing the current NIAP process, including validators and lab personnel, as well as NIST and NSA personnel;
4. **Producers (Large and Small) –** Developers of IA or IA-enabled software that may be subjected to evaluation requirements, including large-scale producers such as Microsoft, IBM, and Oracle, as well as small business concerns;
5. **Governance –** Individuals who are instrumental in making policy and mandating requirements for their agencies, such as heads of NSA and the NIAP or Federal agencies;
6. **Defense Critical –** Individuals who are involved with the operational capabilities of the commands of the armed services, as separate from branches of government such as NASA, FAA, etc.; and
7. **Intelligence –** Individuals who are involved in intelligence gathering activities.

Several of these categories are specialized and crosscut the larger categories along different dimensions. The individuals were assigned to the category that most closely fit their responsibilities. (Several people represented multiple categories, but their input was counted only once.) The purpose of setting up these categories was to ensure that some coverage of input from these perspectives within the community was solicited. They did not restrict in any way the topics discussed or the issues raised in the interviews, at the forum, or in response to the *Federal Register* announcement.

As discussed in Chapter 2, the Critical Infrastructure (CI) community was not considered a separate stakeholder class. The need for CI participation in considering the NIAP changes, however, was raised in interviews and at the forum. An issue concerning CI is the need for Federal mandates or guidance and the right of commercial entities to determine their own courses of action. The Non-DoD Federal Government category covers the CI community for the purpose of collecting input for this study.

The data collected represents a sample of members from each of the stakeholder classes. The intent was to be thorough and ensure representative sampling. No attempt was made to justify any of the findings by statistical analyses.

5.1.2 Interview process

A total of 45 interviews were conducted. There was no attempt to get a statistically significant sample, and interviews were used in conjunction with other source data in a "discovery" process for developing issues. A list of over 300 potential interview candidates across all stakeholder classes was compiled. In March 2004, 100 selected

candidates were mailed letters describing the NIAP study and asking for participation in interviews. Selection was based upon their specific interest in product evaluation as perceived by the analysis team. Based on responses received, interviews were scheduled and conducted. Additional interviews were arranged to ensure that at least three representatives from each stakeholder class were interviewed.

Interviews were conducted either in person or over a speakerphone. Each interview lasted approximately one hour. At the beginning of each interview it was explained that, although notes were being taken during the interview, the interview itself was not for attribution. The interview was not recorded. The interviewee was presented a brief overview of the study's objectives and methodology. The initial questions covered the interviewee's current responsibilities to determine which stakeholder class they represented. Where it was appropriate, some interviewees were assigned more than one stakeholder class. Interviewees were asked for their personal opinions and perceptions rather than "official" or "corporate" positions.

Interviews were free-ranging and concentrated on areas in which the interviewee exhibited some expertise or expressed an opinion. Each interview started with questions on general topics in order to draw from the interviewee issue areas of interest to them. Follow-up questions addressed specific topics and issues raised by the interviewee. Interviews did not contain the same questions, only topics, and the purpose was to raise issue areas, not conduct an opinion poll. Summary sheets were produced for each interview. The following is a sample of the general questions used in the NIAP stakeholder interviews:

1. Are you familiar with the NIAP program/process?
2. Do you use evaluated products?
3. Are you aware of the mutual recognition agreements the United States has with evaluations performed in other countries?
4. Are you satisfied with the current evaluation process?
5. What does *assurance* mean to you?
6. What does a *certificate* mean? What should a certificate mean?
7. How do C&A and product evaluation work together (or not)?
8. How much should the process of evaluation/certification cost? How should the costs be paid? Who should bear the costs?

A total of five IDA personnel participated in conducting the interviews, with at least two participating in each interview. This served to ensure that all essential questions were covered and that notes from each interview were complete. The IDA personnel were chosen based upon their knowledge, background, and availability. The interviews were then analyzed for inclusion in the study.

5.1.3 Forum Data Collection

On October 22, 2004, IDA conducted a NIAP Forum at its Alexandria, Virginia, facilities. Over 150 people, from government and industry, were invited to attend. The purpose of this forum was to provide the greater NIAP community with the opportunity to voice their issues, concerns, ideas, and complaints regarding the NIAP process as it pertained to them.

Approximately 45 people representing government, industry, the NIAP evaluation labs, and the NIAP validators attended the forum. The initial presentations from IDA personnel depicted the methodology utilized in the conduct of the NIAP review. After this brief introduction, the floor was opened to audience participation, and group discussions were held for the remainder of the day.

Areas discussed were:

1. IDA NIAP Review Overview;
2. The NIAP Policy Overview – Statutes, policies, and procedures affecting the NIAP;
3. Existing NIAP Practices – The current state of the NIAP and how it has evolved;
4. Stakeholder Expectations/Data Gathering – The interview process; and
5. Other topics (no topic was out of bounds).

Considerable feedback was received from the attending group, and many of the items discussed were captured in the tables of expectations in section 5.3.

5.1.4 *Federal Register* Announcement

In early November 2004, IDA, in consultation with DHS and DoD filed a Notice in the *Federal Register* on behalf of DoD and DHS to provide all interested parties the opportunity to voice their concerns, issues and ideas on the NIAP process. This was a last attempt to solicit input from interested parties that may not have been reached by the other means discussed in this chapter.

After a review of written material and various statutes on the subject, IDA staff attended a briefing on the issue at the offices of DoD Washington Headquarters Services (WHS) on December 8, 2004. The initial advice of the WHS staff was to approach the task as an information collection pursuant to the requirements found in the Paperwork Reduction Act (PRA). After further research and consideration, it was proposed to WHS that the Notice be considered a Notice for General Solicitation of Comments and not a collection under PRA. This approach was approved.

"The General Solicitation of Comments from the General Public on Review of the National Information Assurance Partnership (NIAP)" was published on Wednesday, February 2, 2005 in *Federal Register* Vol. 70, No. 21, page 5420. The notice required

that comments be submitted in electronic form to DoD/DHS at NIAPReview@ida.org or in written form to the Institute for Defense Analyses on or before March 4, 2005.

A total of 76 comments were received and processed as described above.

5.1.5 Literature Search

The final source of data on expectations was undertaken as a literature search from significant parties such as the Government Accountability Office (GAO), The National Cyber Security Partnership, and others as outlined in Annex A. The text was not parsed, but conclusions and recommendations in these reports were gleaned for the analysis. A total of 18 additional expectations were added to the analysis list.

5.2 Analysis Process

The notes from each interview, remark, and publication were translated into statements of expectations and observations. These statements were collected into an expectations matrix, which was used to synthesize issues across all stakeholder classes. The rules for synthesis of interviews were as follows:

- Each of the interviewers agreed that the final set of expectations and observations recorded from each interview accurately reflected what they heard. In many cases, the statements are not the exact words expressed by interviewees or in written material; the issues were paraphrased for accumulation purposes.
- Statements were reviewed for appropriate labeling, consistent terminology, and characterization as an expectation or an observation.
- Similar expectations were melded within the interview set and across other forms of input.
- Unique instances of expectations not corroborated by at least one other source were considered outliers and dropped. (At least two sources were needed to include the result.)
- Expectations are often conflicting and reveal a basic misunderstanding. No harmonization or resolution of conflicting expectation was undertaken in this chapter.
- Each expectation could be considered a finding; however, findings were reserved for synthesized results of combinations of expectations and observations. As a result, not all topic areas included findings.

This process resulted in a total collection of 1,093 statements from all sources.

5.2.1 Topic Areas

The collection of statements from all sources were then categorized and assigned the following topic areas (topics are not the same as questions asked or areas covered but were derived from the responses):

1. Consumer knowledge and understanding of evaluations;
2. The meaning of a product evaluation certificate;
3. Protection profiles;
4. Evaluation personnel and evaluation laboratory issues;
5. Testing of products in evaluations;
6. Alternate forms of assurance;
7. Relationship between C&A and product evaluation;
8. Mutual recognition, commercial viability, and related issues;
9. Research areas;
10. Target of evaluation (TOE) versus product evaluation;
11. Assurance maintenance;
12. Cost and time issues;
13. NSTISSP-11;
14. Critical infrastructure;
15. Nefarious and malicious behavior in code; and
16. Comments concerning NIST.

The list of topics areas was refined iteratively with the collected expectations and observations. The results collected for each of these areas is presented in the sections below.

5.3 Expectations, Observations, and Findings

This section summarizes the expectations and observations identified in stakeholder interviews, derived from written material provided by interviewees, notes taken and written inputs received at the NIAP forum, notes taken during the literature review, and inputs received in response to the announcement in the *Federal Register.*

Tables 2 through 17 document the expectations and observations. An expectation was associated with an interviewee's delineation of how the system should work. All others were tagged as observations. Each expectation or observation in these tables is identified by its topic area and a sequence number. The second column (description) contains the statement of expectation or observation. The third column shows how many times the expectation or observation was reported during interviews. Since interviewees were not proficient in all areas and follow-up questions were restricted to expertise or opinion areas, the number cannot be normalized but does provide a relative strength measure. Confirmation of these issues by written input to one of the calls for data or in a literature search is indicated by a diamond (♦). In the case of no numeric entry, the issue was not raised during interviews but came from one of the alternative sources. This

approach was taken because interviews allowed for follow-up questioning and may be related to some of the other sources. The additional data sources were not classified by stakeholder classes because in many cases the stakeholder classes were unknown. The remaining columns are shaded to identify the stakeholder class or classes making that statement. In some cases, the number of stakeholder classes exceeds the number of interviewees raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class, indicated by an asterisk (*). Findings that summarize *significant* expectations are presented below in each table where appropriate. At the beginning of each section we summarize the general observations of the interviewers.

5.3.1 Consumer Knowledge and Understanding of Evaluations

The first topic area is the consumer's knowledge about evaluation processes and their understanding of evaluation results. Table 2 shows a broad consensus on several expectations and observations. The first entry shows the strongest agreement (the expectation expressed by the largest number of sources), which was that *interpreting current evaluation results requires a much deeper understanding than most consumers have.* At the same time, a large number of sources expressed the expectation that interpreting evaluation results should require no more than a general understanding of the concepts. Sources from all stakeholder classes observed that the concept of assurance as embodied in evaluations and CC terms in general are not well understood.

Most consumers are knowledgeable about their systems and their security requirements (and usually have deeper expertise available). However, current evaluation practices require a consumer who is knowledgeable, not only about security, but also about a number of evaluation nuances. Not many consumers have the necessary expertise, and even under ideal circumstances, few can be expected to gain it. Most consumers have too many other complex duties to become experts in evaluation.

Table 2. Consumer Knowledge and Understanding – Expectations and Observations

Tracking Code.	Description	Occurrences	Stakeholder Category: DoD	Fed Non DoD.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
EKn-1	Understanding current product evaluation results requires in-depth knowledge of evaluation practices and the arcane terminology of the CC – knowledge that relatively few people have.	31♦	■	■	■	■	■	■	■
EKn-2	People with only a general understanding of evaluation practices and minimal familiarity with CC terminology should be able to read and understand evaluation results.	18	■	■	■	■	■	■	■
EKn-3	NIAP currently provides training for evaluators. NIAP should also be funded to train consumers in evaluation processes and interpretation of results.	15♦	■	■	■	■	■	■	
EKn-4	Education is a responsibility at all levels.	2♦			■	■			
Observations									
OKn-1	The concept of assurance specifically and CC terms in general are not well understood.	15	■	■	■	■	■	■	■
OKn-2	We are not likely to get many consumers who fully understand evaluation practices and are fluent in CC terminology.	7♦		■	■	■	■	■	■
OKn-3	Not every consumer, producer, or manager has to be an evaluations expert. One knowledgeable person can advise a group.	4♦		■	■		■		
OKn-4	There is no need for consumers to be knowledgeable about evaluations.	4	■	■			■		■

Notes: * Indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.

♦ Issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Consumer Knowledge and Understanding	
FEKn-1	Consumers need a better understanding of information assurance threats and protection methods, and a basic understanding of NIAP evaluation processes to interpret evaluation results and make informed decisions about product suitability for their needs. Supported by (table above): Knowledge and Understanding Expectation 1 [EKn-1] Knowledge and Understanding Observation 1 [OKn-1] Knowledge and Understanding Expectation 2 [EKn-2]
FEKn-2	Evaluations are often reported in technical CC terms and do not state in plain language what information assurance protection the product provides. Supported by (table above): Knowledge and Understanding Observation 1 [OKn-1] Knowledge and Understanding Expectation 2 [Ekn-2] Knowledge and Understanding Finding 1 [FEKn-1]

5.3.2 Certificate Meaning

Given that consumers are not evaluation experts, the certificate itself needs to make the information it conveys more easily understood.

Table 3 shows that respondents in all stakeholder groups thought *evaluation certificates should accurately characterize the types of protection provided by the product and how it was tested.* They also want to see an assessment of the types of

applications for which the product is considered suitable. If a product is evaluated as a firewall, for example, then the evaluation should say that it is suitable for that task. In most cases, consumers who are not evaluation experts are not able to research the material behind current evaluation certificates to determine whether the product meets their needs. As a result, many equipment buyers in the DoD consider an evaluation certificate a "check box" in their purchase decisions, required independently of the protection provided by the product or its suitability for the intended use.

The meaning of a certificate would also be enhanced if it cited the product's conformance to a well-crafted protection profile (PP). (DoD provides for this by requiring the security target (ST) to be based upon an approved PP where one exists.) To support this objective, each such PPs will have to address the core capabilities of a relatively broad class of products; for example, firewalls. A further improvement in certificates would be a scheme for grading the security provided by a product such as home use, commercial use, or national security use. At present, certificate descriptions of assurance and strength of function are meaningful to only a small number of evaluation experts.

Table 3. Certificate Meaning – Expectations and Observations

			Stakeholder Category						
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ECm-1	Evaluations should accurately characterize the types of protection provided by the product and how it was tested.	23♦	■	■	■	■	■	■	■
ECm-2	Evaluations should accurately characterize a range of suitable uses for the product.	19	■	■	■	■	■	■	■
ECm-3	Certificates should identify additional documentation that is available to allow knowledgeable consumers to assess the product's suitability for their use.	4			■		■	■	
Observations									
OCm-1	Most DoD buyers consider a certificate the essential factor, independent of the protection provided or the product's suitability for use.	7	■		■	■	■	■	
OCm-2	Current certificates do not rate a product's claims or suitability for use.	2♦		■			■		
OCm-3	If we had protection profiles (PPs) for core capabilities, certificates of compliance could provide a measure of suitability for use.	2*♦			■	■		■	■
OCm-4	Certificates should not attempt to rate a product's security or suitability for use.	2*			■		■	■	
OCm-5	The consumer wants some kind of independent statement that states the goodness of the product (like a UL certificate).	2♦			■	■			

			Stakeholder Category						
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
OCm-6	There is no way to rescind an evaluation certificate for a flawed product	♦							
Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class. ♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)									

Findings – Evaluation Certificates	
FECm-1	Evaluation certificates in general do not identify the degree of security provided by the product or provide example applications for which the product is suitable. Supported by (table above): Knowledge and Understanding Finding 1 [FEKn-1] Certificates Expectation 1 [ECm-1] Certificates Expectation 2 [ECm-2]

5.3.3 Protection Profiles

A protection profile (PP) is a set of specifications (both functional and assurance) against which a product may be evaluated. Anyone may write a PP, but there are no requirements for evaluations to claim conformance to any PP. A properly vetted PP would represent the requirements of a class of stakeholders for a product type or product area. NSA developed most of the present PPs for DoD usage, although consortiums have also developed a few (such as SMARTCARD). PPs prevent removing claims from an ST and ultimately result in improved security.

As Table 4 shows, opinion on PPs was divided. The larger group believes that conformance to PPs should be required. (DoD provides for this by requiring the ST to be based upon an approved PP where one exists.) A smaller group, however, did not want to require conformance to PPs. Producers, in particular, would prefer not to be held to standard, vetted protection profiles. Other stakeholders also expressed the opinion that verifying target of evaluation (TOE) claims (the current alternative to PPs) is adequate.

Including testing requirements in PPs was surprisingly popular, except among the DoD stakeholder class. Adding test requirements to a PP would be additional work for the writers of PPs. A uniform set of tests, however, would make testing much more consistent across evaluation laboratories.

Focusing PPs on core capabilities, and avoiding non-essential (proprietary) features, would allow a wider range of products to meet the conformance requirements.

Table 4. Protection Profiles – Expectations and Observations

Sequence Num.	Description	Occurrences	Stakeholder Category: DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
	Expectations								
EPP-1	Conformance to one or more trusted PPs should be required.	20♦	■	■	■		■	■	■
EPP-2	Protection profiles should include a definition of the testing required to satisfy conformance.	20		■	■	■	■	■	■
EPP-3	Protection profiles for core capabilities should be developed to avoid PP proliferation.	7♦	■	■	■	■			■
EPP-4	Demonstrating product conformance to one or more protection profiles should not be mandated. Verifying TOE claims is sufficient.	5	■	■	■	■	■	■	
	Observations								
OPP-1	Protection profiles should be used as a means to consolidate community interests, expertise, and support.	20♦	■	■	■	■	■	■	■
OPP-2	Conformance to a protection profile serves as a measure of suitability for use. PPs can also aid product design.	7		■	■	■			
OPP-3	NIST is better equipped to get a consensus PP.	6♦		■	■	■	■		
OPP-4	Poorly conceived and unstable PPs have contributed to a reluctance to develop and use them.	5♦	■			■	■		
OPP-5	The PP needs to be produced by the government and widely vetted.	4				■	■		
OPP-6	NSA is the proper entity to write PPs for government use.	3	■						
OPP-7	PP's contain useful information to state requirements, but do not work as evaluation criteria.	2♦		■					
OPP-8	PP development process should be a lot faster.	2	■		■				
OPP-9	Producer has paid lab to develop a core capabilities PP for their own internal use.	2				■			
OPP-10	PPs should not be wish-lists	♦							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Protection Profiles	
FEPP-1	Protection profiles covering core information assurance capabilities for general use have not been developed. A number of protection profiles that address the higher levels of assurance for national security systems have been developed by NSA for use by that community. Protection profiles for capabilities that satisfy more modest assurance requirements have not been developed. Supported by (tables above): Certificates Finding 2 [ECm-2] Protection Profiles Expectation 4 [EPP-4]

5.3.4 Evaluation Personnel and Lab Expectations and Observations

The principal issues regarding evaluation personnel and laboratories were the apparent conflict of interest in labs preparing evidence and conducting the evaluation for the same product, and certification of evaluators (see Table 5). One group thought labs should be restricted from preparing evidence for the evaluations they conduct. Another, roughly equal-sized group thought that labs could keep these responsibilities separate and ensure there was no conflict of interest.

Certification of evaluation personnel was recommended as a means to gain consistency in evaluations across laboratories. A certification program is not available and needs to be developed. The perceived high turnover at labs was cited as contributing to inconsistency.[20] Certification of validators overseeing evaluations was also recommended. Calling for U.S. citizenship does not seem reasonable in light of Mutual Recognition Agreements (MRA).

Process stakeholders thought that government oversight was intrusive. In contrast to other accreditation programs that NIST and NVLAP run, this is the first standard that requires such a high degree of government oversight in detail for each evaluation. The Cryptographic Module Validation Program (CMVP, FIPS140) provides some government oversight, but not to the extent the CCEVS requires. This level of oversight should, however, contribute to evaluation consistency.

Table 5. Evaluation Personnel and Lab – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
EPe-1	There is an apparent conflict of interest between preparing evidence for an evaluation and conducting an impartial evaluation. Labs should not prepare evidence for evaluations they conduct.	11	■	■	■	■	■	■	■
EPe-2	Personnel performing evaluations should be formally certified as NIAP evaluators.	12	■	■	■	■	■		■
EPe-3	Personnel overseeing evaluations should be formally certified as NIAP validators.	11	■	■	■	■	■		■
EPe-4	A single lab can provide both evidence and the evaluation, but they need to separate responsibilities so a conflict of interest does not exist. (The amounts of talent and market impact were cited as issues).	10			■	■	■		■
EPe-5	Evaluation results must be repeatable across labs and among products.	6	■		■	■			

[20] Although high turnover rate was discussed among several interviewees, we do not have data to support the contention.

			Stakeholder Category						
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
EPe-6	There should be no appearance of conflict of interest in any aspect of evaluations.	5							
EPe-7	U.S. labs should require U.S. citizenship for evaluation.	4							
	Observations								
OPe-1	Oversight is intrusive, delegate responsibility.	4							
OPe-2	The evaluation process is not consistent and repeatable between labs.	3♦							
OPe-3	High personnel turnover rates at labs degrade evaluation performance.	3							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Evaluation Personnel	
FEPe-1	Product evaluators come from a variety of disciplines with varying levels of expertise. Although NIAP checks that evaluation processes are followed correctly, no process has been established to ensure adequate training of evaluators and validators. Supported by (table above): Evaluation Personnel Expectation 2 [EPe-2] Evaluation Personnel Expectation 3 [EPe-3] Evaluation Personnel Expectation 5 [EPe-5] Evaluation Personnel Observation 2 [OPe-2] Evaluation Personnel Observation 3 [OPe-3]
FEPe-2	Current conflict of interest rules, particularly those that allow laboratories to develop evidence and conduct evaluations on the same products, are open to potential abuse. Supported by (table above): Evaluation Personnel Expectation 1 [EPe-1] Evaluation Personnel Expectation 6 [EPe-6]

5.3.5 Testing of Products in Evaluation

There was general agreement that product evaluations need to include more testing to meet the security assurances sought. DoD PPs often add the AVA_VLA.3 assurance requirement (called plus-up by several interviewees) to increase the amount of vulnerability testing being performed. Expectations on providing tools and requiring source code review came from all stakeholder classes (see Table 6). Automated tools find many common mistakes that can occur during software coding (open ports, buffer overflows, obvious Trojan horses, and backdoor entries). In order for tools to have maximum value, they need to be standardized, portable, and freely available. Some process of certification by the laboratories needs to be developed to ensure that the current and certified copies of tools are used in evaluations. However, general open availability would encourage the developers to use the tools *before* evaluation, thus shortening evaluation iterations and saving time.

Automated source code review is more reliable than testing at finding buffer overflows and some forms of malicious code, as well as apparently benign backdoors left by programmers. To avoid the potential exposure of proprietary intellectual property in source code, it was suggested that producers run their own (automated) source code review and submit the results to evaluators.

A small minority suggested that they would prefer making it easier to conduct evaluations, encouraging evaluation of more products, rather than making it harder by increasing testing requirements. In fact, tool usage could be applied to products that are not normally thought of as IA or IA-enabled but have an impact on system security.

Table 6. Testing of Products in Evaluation – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ETe-1	A sanctioned set of automated analysis tools is needed to increase trust in evaluation results. These tools should be funded by the government and made available to all.	23♦	■	■	■	■	■	■	■
ETe-2	Product evaluation at all levels must include source code review.	12	■	■	■	■	■	■	■
ETe-3	All evaluations should include vulnerability testing.	7♦			■	■	■		■
ETe-4	The CEM should specify testing requirements in detail and provide example test cases for each functional requirement.	6			■		■	■	
ETe-5	Evaluations below EAL4 need to include more testing.	8♦		■	■	■	■	■	■
ETe-6	Producers should be required to provide automated source code review as evidence.	3			■	■	■		
Observations									
OTe-1	Adding testing requirements to evaluations below EAL4 is not necessary.	3	■			■			
OTe-2	Evaluations should not require that labs be given access to the producer's source code.	3	■			■	■		
OTe-3	Testing in evaluations needs to be automated.	2♦				■			
OTe-4	Moving testing requirements down to lower EAL levels is not the right thing to do. Evaluating more products to raise the overall level of assurance is more appropriate.	2*	■		■			■	■
OTe-5	Automated testing tools would raise the confidence and trust in the results produced.	2♦	■				■		
OTe-6	Evaluations below EAL5 are a waste of time.	2				■			■

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Testing	
FETe-1	Automated tools can help standardize evaluation processes, perform more thorough product analyses, and reduce evaluation costs. No standard collection of automated security analysis tools has been developed or assembled to support evaluations. Supported by (tables above): Testing Expectation 1 [ETe-1] Testing Observation 3 [OTe-3] Testing Observation 5 [OTe-5] Knowledge and Understanding Finding 2 [FEKn-2]
FETe-2	Both the Common Evaluation Method (CEM) and protection profiles often omit detailed testing requirements. Supported by (tables above): Testing Expectation 3 [ETe-3] Testing Expectation 5 [ETe-5] Protection Profile Expectation 2 [EPP-2]
FETe-3	No automated review of source code is required for evaluations at EAL4 and below. For software products, the code represents a complete technical specification of the product's functionality, and is much more revealing than the other design and implementation documentation that is considered in evaluations. Automated source code review could screen out many common security flaws that currently go undetected. Supported by (table above): Testing Finding 1 [FETe-1] Testing Expectation 2 [ETe-2] Testing Expectation 6 [ETe-6] Testing Observation 5 [OTe-5]

5.3.6 Alternate Forms of Assurance

Table 7 shows that alternate forms of assurance are not significant concerns for most stakeholder classes. Alternate forms of assurance, however, may reduce costs and could be useful at lower evaluation assurance levels. Several interviewees believed that alternative assurance methods are needed, especially to reduce costs (such as a "CC lite"). This is the case for organizations or situations that cannot afford to pay for evaluations, such as many small web applications, small businesses, and open source software (OSS) projects. Support for alternative assurance levels was strongest for use in lower assurance evaluations. Many believed that NIAP evaluation would be strengthened if the alternative assurance methods were used to supplement the NIAP evaluation, with SSE, CMM, and CMMI specifically mentioned as examples of alternative assurance methods. These assurance methods would augment (not replace) the current assurance methods. These alternatives are discussed in detail in Chapter 6.

Table 7. Alternate Forms of Assurance – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
EAa-1	Alternate forms of assurance are needed (beside current NIAP evaluations) to reduce costs (for example, for small businesses).	7♦			■	■			
EAa-2	Phase in CMM and/or CMMI System Security Evaluations (SSE) in place of current NIAP processes.	2				■			
EAa-3	Need a Common Criteria 'lite' with alternate forms of assurance and less cost.	2♦			■	■			
EAa-4	Best Practices should be incorporated.	♦							
Observations									
OAa-1	Supplementing product evaluation with alternate forms of assurance (such as an SSE CMM/CMMI) would improve product assurance.	8♦	■		■	■	■		■
OAa-2	Alternate forms of assurance should be researched and considered in evaluation. Alternate forms of assurance could be used in cases where evaluation is not timely, appropriate, or cost effective.	2♦			■		■		
OAa-3	Alternate forms of assurance are not needed and will only cloud the issue.	2		■	■				

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.3.7 Relationship between C&A and Product Evaluation

Certification and accreditation of systems was considered essential by all stakeholder classes, whether or not product evaluations are involved. Product evaluations can help C&A and should be taken into account. In fact, it was recommended that both FISMA and DITSCAP C&A guidance be revised to include requirements for using evaluated products (see Table 8).

Table 8. Relationship between Certification and Accreditation (C&A) and Product Evaluation – Expectations and Observations

Sequence Num.	Description	Occurrences	Stakeholder Category: DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ECa-1	C&A for security systems is an absolute requirement.	28	■	■	■	■	■	■	■
ECa-2	DITSCAP and FISMA C&A requirements should be modified to include evaluated products.	14	■	■	■	■	■	■	■
ECa-3	DITSCAP and FISMA should impose uniform requirements for the use of evaluated products.	8		■	■		■		■
ECa-4	Product evaluation is a required part of C&A.	2	■		■				
ECa-5	Product evaluation data should be made available for C&A	♦							
Observations									
OCa-1	Use of evaluated products should add value to C&A.	10	■		■	■	■		
OCa-2	A good solution to composability[21] will not replace C&A but can assist it.	5*	■	■	■	■	■	■	
OCa-3	C&A is sufficient by itself. Product evaluations add no value.	3		■			■		
OCa-4	C&A should be able to reuse evidence from product evaluations, allowing C&A to concentrate on interfaces.	2		■	■				

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – C&A	
FECa-1	Certification and accreditation of systems was considered essential by all stakeholder classes, and product evaluation should improve C&A Supported by (table above): C&A Expectation 1 [ECa-1] C&A Expectation 2 [ECa-2] C&A Expectation 5 [ECa-5] C&A Observation 1 [OCa-1]

5.3.8 Mutual Recognition, Commercial Viability, and Related Issues

There was a consensus from all stakeholder classes on the need for mutual recognition agreements, as shown in Table 9. Differences in evaluation schemes used in different countries, which lead to inconsistent evaluations, however, were raised as an

[21] Composability – refers to the problem that combining products with well-established security properties can produce systems with significant security flaws. How to detect these flaws in systems built from secure components is not yet solved.

issue. Some suggested that the limit on current agreements (EAL4 and below) could be raised to EAL7.

Opinions on the importance of commercial viability of evaluations – that is, sufficient public demand for evaluated products to sustain the NIAP evaluation process without government support – were mixed.

All stakeholder classes thought that by some means shifting liability for cyber losses away from the consumer would help the commercial viability of evaluations. This would mean that producers, evaluation labs, the Government, or some combination would have to stand behind evaluated products and warrant them against certain types of loss. If evaluations do not provide sufficient added assurance to reduce consumers' liabilities, consumers will not see any value in evaluation processes and will not pay any extra premium for evaluated products.

Table 9. Mutual Recognition, Commercial Viability, and Related Topics – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
EMR-1	Mutual recognition is necessary.	20♦	■	■	■	■	■	■	■
EMR-2	Evaluations must be consistent (repeatable) across labs, including labs in other countries. At present, different countries have adopted different evaluation schemes and these are not seen as equivalent.	9♦	■		■	■	■		■
EMR-3	Commercial viability is necessary.	7♦			■	■	■		
EMR-4	Commercial viability is not necessary.	4	■			■	■	■	■
Observations									
OMR-1	Consumers typically have to assume liability for any information assurance losses. If evaluated products came with warranties against such losses, it would give them a commercial advantage over unevaluated products.	9	■	■	■	■	■	■	■
OMR-2	Current MRA's are limited to EAL4 and below. This limit should be raised to EAL7.	6♦		■	■	■	■		■
OMR-3	In spite of MRA's, not all product evaluations at EAL4 and below are accepted country to country.	2♦			■		■		
OMR-4	There is no need to change EAL limits in MRA's (up or down). The limits are good where they are.	3			■		■		■
OMR-5	Under the current paradigm NIAP evaluations cannot be made commercially viable.	2♦			■				

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Mutual Recognition Agreements	
FEMR-1	NIAP has not addressed warranty or liability issues for evaluated products. No legal or business-case analyses on who might underwrite warranties for evaluated products was found, or what effect warranties might have in promoting adoption of evaluated products. Supported by (table above): MRA Observation 1 [OMR-1]
FEMR-2	Mutual Recognition is necessary. Supported by (table above): MRA Expectation 1 [EMR-1]

5.3.9 Research Areas

The NIAP as originally chartered intended to support tool development, research, and evaluations (see Section 3.1). The burden of developing evaluation processes, setting up labs, etc., has become so great that few resources are left to devote to research and tools. Sorely lacking are metrics that both quantify security aspects of software programs and the effectiveness of evaluations. Several respondents suggested that the NIAP's research focus should be restored (see Table 10).

A particularly difficult problem is how to combine product metrics to compute a system's overall security posture. This problem is called composability. While composability was recognized as a problem, there were mixed opinions on whether it could be solved or whether the solution would have sufficiently wide applicability to make it worth the effort.

Table 10. Research Areas – Expectations and Observations

			Stakeholder Category							
Sequence Num.	**Description**	**Occurrences**	**DoD**	**Federal Gov.**	**Process**	**Producer**	**Governance**	**Defense Critical**	**Intelligence**
Expectations									
ERe-1	NIAP should support research into assurance metrics, composability, and return on investment.	7♦	■	■	■		■		
ERe-2	Research is needed to develop measures of product assurance and evaluation effectiveness so that consumers can compare products and evaluation results.	4♦	■		■				
Observations									
ORe-1	A set of security metrics is lacking.	5♦			■		■		
ORe-2	Composability is solvable; research is needed to produce the solution.	4			■	■			
ORe-3	Composability is not solvable and should not be pursued.	3	■		■		■		

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Research	
FERe-1	A number of open research problems remain unaddressed, including assurance metrics and solutions to composability among other security problems. Supported by (table above): Research Expectation 1 [ERe-1] Research Expectation 2 [ERe-2] Research Observation 1 [ORe-1]

5.3.10 Target of Evaluation (TOE) Versus Product Evaluation

An expectation expressed by all stakeholder classes was that evaluations should be conducted on products as delivered and as used in normal environments, not on specially configured targets of evaluation (TOE). The products are what consumers buy and use, not the TOEs. A smaller group, which did not include producers, expressed the opinion that evaluating TOEs against specific claims meets particular needs and is acceptable if you understand the fine print in the certificate.

Table 11. TOE Versus Product Evaluation – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ETOE-1	Product evaluation must be for the product as delivered (not TOE).	12♦							
Observations									
OTOE-1	TOE evaluations are acceptable do not need product evaluations.	6							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings – Targets of Evaluation	
FETOE-1	A number of products have been evaluated in unusual configurations and environments that do not represent consumers' general use. These evaluations do not provide sufficient information to determine how these products will perform in typical system configurations and normal use. Supported by (tables above): TOE Expectation 1 [ETOE-1] Knowledge and Understanding Expectation 1 [EKn-1] Knowledge and Understanding Expectation 2 [EKn-2] Knowledge and Understanding Observation 1 [OKn-1] Knowledge and Understanding Finding 1 [FEKn-1]

5.3.11 Maintenance Assurance

Producers often create new releases of products with defect corrections and minor functional enhancements. At present, the standard CC assurance packages for EAL1

through 7 have no provisions for accommodating such changes. While maintenance assurance and flaw remediation packages are part of the standard, they are not part of any assurance packages. Deviations from the standard assurance packages are seldom made. One exception is the case where PP conformance is claimed and the PP requires maintenance assurance. Each new release is therefore treated as a new product, requiring full evaluation. A number of stakeholders felt that analysis and testing of minor product changes, which would require considerably less effort than a full evaluation, should be sufficient to extend the original certificate to cover the updated product. These provisions occur within the maintenance assurance packages. Further, it is expected that where security issues are involved, security failures and the patches to improve the product should be accompanied by notification to all registered users. These provisions occur in the flaw remediation packages. DoD may handle this in individual procurements as an acquisition issue or directly in the PPs, but the more formal maintenance assurance and flaw remediation would provide increased uniformity to DoD and a measure of protection to all stakeholders. Both the CC and the CMVP have approaches for revalidation that address the type of change to a product. They simply need to be part of the EAL packages.

Table 12. Assurance Maintenance – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations										
EAM-1	When changes are made to a product (either for feature enhancement or to correct defects), a process is needed to validate the changes and extend its certificate, short of full re-evaluation.	10♦							
EAM-2	Flaws in commercial products should be looked at (flaw remediation should be part of maintenance assurance, and both should be required).	♦(strong input)							
Observations										
OAM-1	Do not recommend a maintenance assurance program.	2							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

Findings –Assurance Maintenance	
FEAM-1	Evaluations should include both maintenance assurance and flaw remediation work packages. Supported by (table above): Maintenance and Assurance Expectation 1 [EAM-1] Maintenance and Assurance Expectation 2 [EAM-2]

5.3.12 Cost and Time Issues

Evaluation costs are too high and they take too long. These are common complaints, particularly from small businesses. The documentation generated for evaluations is partly responsible. While no specific documentation is listed in the CC, information presentation and content result in the development of evaluation-specific documentation. Little of this documentation is part of normal development processes. This documentation is expensive to produce and often requires revision to satisfy evaluators. While this documentation may be required at higher assurance levels, large parts of the information required are present in developer documentation. The need for specific documentation is not present in the CC, only content. Many developers are either convinced to provide separate documentation, or prefer to do so for proprietary reasons. The CCEVS should stress that content is the important part of the documentation process, leaving its interpretation to the evaluation laboratories. The labs frequently mandate the specific format/structure of the documentation.

Table 13. Cost and Time Issues – Expectations and Observations

			Stakeholder Category							
Sequence Num.	**Description**	**Occurrences**	**DoD**	**Federal Gov.**	**Process**	**Producer**	**Governance**	**Defense Critical**	**Intelligence**
Expectations									
ECT-1	The government should subsidize evaluations of products that are used in highly classified applications and/or have limited application.	2♦			■	■			
ECT-2	DoD should pay for the product evaluation of any product it is considering using and let the market benefit from that expenditure.	2♦				■	■		
ECT-3	Evaluation times should be considerably less than product release cycles.	♦							
Observations									
OCT-1	Evaluation costs are too high.	14♦	■	■	■	■	■	■	■
OCT-2	Evaluations take too long.	9♦	■	■	■	■	■	■	■
OCT-3	Under the current process, small companies are at a real cost disadvantage when it comes to product evaluations.	7♦	■			■	■		

OCT-4	Current practices produce voluminous, uninformative documentation that is a burden to all. Documentation needs to be written in plain language and streamlined.	8♦							
OCT-5	Evaluation costs are acceptable.	3							
OCT-6	The time evaluations take is acceptable.	3							
OCT-7	We should not be concerned that some producers consider evaluation costs a barrier to entry. They are a cost of doing business.	3							
OCT-8	The government should help small businesses with training and subsidies for evaluations.	3♦							
OCT-9	Documentation requirements are right and proper.	2							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.

♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.3.13 NSTISSP-11

Comments relating to NSTISSP-11are included here for completeness (see Table 14). These comments are not significant in number and provide no usable data.

Table 14. NSTISSP-11 – Expectations and Observations

			Stakeholder Category						
Sequence Num.	**Description**	**Occurrences**	**DoD**	**Federal Gov.**	**Process**	**Producer**	**Governance**	**Defense Critical**	**Intelligence**
Expectations									
EN11-1	NTISSP-11 should specify a cost threshold for products requiring evaluation. Evaluation of inexpensive items is not cost effective.	2							
EN11-2	A collection of protection profiles is needed before NTISSP-11 can be effectively applied.	3♦							
Observations									
ON11-1	NTISSIP-11 is not well written.	3♦							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.

♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.3.14 Critical Infrastructure

An expectation expressed by stakeholders from all classes was that the Critical Infrastructure Protection (CIP) community should be brought under the national security mandates. Most government departments and agencies that are part of CIP are already under the FISMA mandates. (See the discussion of policy issues in Chapter 3.) However, including CIP under product evaluation and CC mandates may create an undue burden of cost. Any inclusion of the CIP should be deferred until a more modestly priced evaluation process can be developed, especially for the lower levels of assurance (EAL3 and below).

However, many of the products that have already been evaluated are at assurance levels more suited to critical infrastructure and the rest of government than to the national security community. These constituencies should be encouraged to make full use of the advantages of evaluated products.

Table 15. Critical Infrastructure – Expectations and Observations

			Stakeholder Category							
Sequence Num.	Description	Occurrences	DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ECI-1	The government should impose information assurance requirements on the nation's critical infrastructure (banking, electric, health, etc.).	11♦							
ECI-2	The government should not impose information assurance requirements on the nation's critical infrastructure (banking, electric, health, etc.).	5							
ECI-3	The concept of a NIAP advisory group representing public (state, local, and commercial) interests or a wider coalition (partnership beyond NSA and NIST) is needed	♦							
Observations									
OCI-1	Current laws and mandates are too spread out. Need one source for all.	2♦							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.3.15 Nefarious and Malicious Behavior

Although there was little input on this subject, malicious code and backdoor access paths inserted during development have to be considered in any assurance arguments. Many of the interviewees felt uncomfortable discussing this area and there was little written input. Tools that examine code and product execution for common security coding areas can also examine the code for some types of these activities.

Table 16. Nefarious and Malicious Behavior Code – Expectations

Sequence Num.	Description	Occurrences	Stakeholder Category: DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ENe-1	Evaluations should include tests for malicious code.	7♦	■	■	■	■			■
ENe-2	Evaluations need not include tests for malicious code.	2					■		■

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.3.16 Comments Concerning NIST

The last areas of concern gleaned from the input materials concerned NIST, and they are presented in Table 17.

Table 17. Comments Concerning NIST – Expectations

Sequence Num.	Description	Occurrences	Stakeholder Category: DoD	Federal Gov.	Process	Producer	Governance	Defense Critical	Intelligence
Expectations									
ENi-1	NIST involvement in NIAP CCEVS is minimal and decreasing.	7	■	■	■	■			■
ENi-2	NIST should take a larger role in the NIAP/ NVLAP process.	2♦					■		■
ENi-3	NIAP should bring in additional partners beyond NSA and NIST.	♦							

Notes: * indicates the number of stakeholder classes exceeds the number of interviews raising the issue. This is due to the fact that some interviewees are placed in more than one stakeholder class.
♦ issue identified in other sources (NIAP Forum, Federal Registry Announcement, or literature search)

5.4 Summary of Issues and Findings

The following statements summarize the 756 recorded expectations from the collection of interviews, forum discussions, and other contributed input. "Issues" represents the principal concerns raised by interviewees, forum participants, and other contributors. "Expectations" represents recommendations expressed by these sources.

5.4.1 Consumer Knowledge and Understanding

1. **Issue**: People with only a basic familiarity of evaluations often do not fully understand what an evaluation says about a product and are not able to determine whether the product meets their needs.

   Expectation [ES-01]: Expanding the NIAP education programs for consumers would alleviate this problem.

2. **Issue**: Evaluations often contain confusing statements about what assurance aspects were evaluated and how the product performed.

   Expectation [ES-02]: Evaluations should state in plain language what information assurance protection the product provides.

5.4.2 Evaluation Certificates

1. **Issue**: Evaluation certificates contain little useful information.

   Expectation [ES-03]: Evaluation certificates should identify the degree of security provided and provide example applications for which the product is suitable.

2. **Issue**: Evaluated products are not required to conform to a well-formed, properly vetted protection profile.

   Expectation [ES-04]: Conformance to a well-crafted, properly vetted protection profile should be made mandatory.

5.4.3 Protection Profiles

1. **Issue**: Available protection profiles focus on special capabilities at higher levels of assurance.

   Expectation [ES-05]: A collection of protection profiles covering core information assurance capabilities at more modest assurance levels should be developed.

5.4.4 Evaluation Personnel

1. **Issue**: There is no requirement for evaluators to demonstrate and maintain their technical competence.

   Expectation [ES-06]: A credentialing program should be developed to ensure adequate training of evaluators and consistent evaluations across laboratories.

2. **Issue**: The conflict of interest rules governing evaluation laboratories and their personnel are weak.

   Expectation [ES-07]: The conflict of interest rules, particularly those for developing evidence and conducting evaluations on the same products, should be reviewed and strengthened.

5.4.5 Testing

1. **Issue**: There is no requirement for the use of code analysis or testing tools in evaluations.

   Expectation [ES-08]: The NIAP should develop and make available a standard collection of automated security analysis tools, and require use of these or equivalent tools in evaluations.

2. **Problem**: At present, the Common Evaluation Method (CEM) and protection profiles require no explicit vulnerability testing in evaluation procedures.

   Expectation [ES-09]: Both the CEM and protection profiles should specify vulnerability testing requirements.

3. **Issue**: Source code review is not required for evaluations.

   Expectation [ES-10]: Review of source code should be required at all evaluation levels. Developers may provide results of automated tool analyses for evaluations at EAL3 and below to avoid giving evaluators access to proprietary code. See Annex F for more information about tools.

5.4.6 Commercial Viability

1. **Expectation [ES-11]:** Market forces would encourage developers and insurers to warrant NIAP-evaluated products and assume at least limited liability for information assurance breaches.

   Issue: No such product warranties have emerged, which implies that either consumers do not see added value in warranted, higher-assurance products, or underwriters do not perceive evaluations as providing sufficient added assurance, or evaluations are not applied widely enough to develop this market.

   Conjecture [CES-1]: Market forces would benefit by strengthened evaluations and wider application of evaluations.

5.4.7 Research

1. **Issue**: A number of open research problems remain unaddressed, including assurance metrics and solutions to composability among other security problems.

   Expectation [ES-12]: The NIAP should support research in these areas.

5.4.8 Targets of Evaluation

1. **Issue**: The Target of Evaluation (TOE) concept allows a developer to tailor what is evaluated, which is often not the whole product or is some unusual configuration of the product.

   Expectation [ES-13]: Whole products should be evaluated in their normal usage configuration and environment.

6. Areas of Concern

This Chapter integrates the findings of Chapter 3, Chapter 4, and Chapter 5 into overall areas of concern from which impacts and recommendations flow. Chapter 7 describes options for implementing these recommendations. The concerns addressed here will need a phased approach to implementation. While tools can reduce costs, they must be developed and their utility demonstrated before their use can be mandated. The roadmaps in Chapter 8 address these timing issues for each option.

6.1 Funding and Priorities

Funding and priority shifts have moved the NIAP away from its original intent. Chapter 3 found that the lack of a formal mandate and budget have limited the scope of the NIAP's activities [FPCy-2]. This, coupled with the explosive growth in evaluations documented in Chapter 4 (Section 4.4), has caused the NIAP to focus almost exclusively on evaluations, which are only part of its intended service [FN-2, and FN-3].

Observation: Stretched NIAP budgets and a shortage of qualified validators have required the NIAP to continually revise and rework its oversight of evaluations.

In Chapter 3, we found that the NIAP is not funding research, tools as originally intended [FPCy-3, FPRe-1, FPRe-3, FPRe-4, FPRe-5], or the derived requirement of education and training [AN-09, AN-17, EKn-1, EKn-2, EKn-3, EKn-4, OKn-1, OKn-2]. The expectations of stakeholders, as discussed in Chapter 5, indicate that the stakeholders believe gaps in security metrics and composability of systems exist. Stakeholders expect the NIAP to support research in these areas [ERe-1, ERe-2].

Budgetary restrictions, as discussed in Chapter 4, have precluded the NIAP from developing education and training resources for IT system consumers, tools to support secure product development, and protection profiles for non-military applications [FN-2]. The expectations of stakeholders, as discussed in Chapter 5, is that the NIAP to needs develop and make available a standard collection of automated security analysis tools, and require the use of these or equivalent tools in evaluations [ETe-1].

6.2 Product Evaluation Focus

The NIAP is currently narrowly focused on product evaluations, which are only part of the overall cybersecurity landscape. They have actually performed well within this limited scope [FN-1, FN-5]. Chapter 3 documented that the requirement for acquisition of evaluated IA and IA-related products currently applies only to the DoD and National Security Systems [FPAq-1]. No tie between the DITSCAP and evaluated products exists.

The rest of the Federal Government has even less guidance on how to choose IT security products and/or integrate them with their certification and accreditation (C&A) programs. Federal statutes and OMB require C&A of many IT *systems*, but they do not require any interaction between the NIAP *product* evaluations and C&A activities [FPAq-2]. C&A is a required activity and will be performed with or without product evaluation. Currently, the results of a product evaluation (evidence, documentation) are not specifically intended for system security certification agents—they are primarily developed for those involved in the evaluation/validation process. To the extent that the NIAP/CCEVS can/does change their documentation and evidence to also meet the needs of system security certification agents (and system auditors, system developers/integrators), these evaluation deliverables will be more useful. In Chapter 5 stakeholders were concerned that the details of analysis and testing results contained in the NIAP evaluation technical reports are not available to DITSCAP and FISMA C&A processes [ECa-2, ECa-3, ECa-5, OCa-1].

6.3 Cybersecurity Changes Since the NIAP Establishment

The cybersecurity landscape has shifted while the NIAP has struggled to keep up with evaluations. The number of evaluations has grown to the point of overtasking the pool of validators [FN-3]; this is amplified by the complexity and confusion of cybersecurity policies and standards [FPCy-1]. In many cases the technology is changing faster than formal standards processes are able to track. This makes it difficult for Government agencies to determine which standards to use [FPSt-1]. Moreover, policies evolve so rapidly, imposing new requirements and superseding each other, that government procurement officials often cannot determine which requirements apply to their particular situation [FPCy-1].

In addition, the Common Criteria (CC) upon which the NIAP evaluations are based has not kept up with changes in the cybersecurity landscape. For example, stakeholders expect more rigorous testing and automated source code review at all levels of assurance [FETe-1, FETe-2, FETe-3, ES-08, ES-09, ES-10]. Other necessary changes to the CC and CCEVS process that were identified include:

- Requiring evaluators to review software source code in depth for security purposes. This review must be automated due to shear volume and complexity [FETe-3]. In the CCEVS, source code is not even available at the lower evaluation assurance levels.
- Requiring the use of automated tools to identify critical code components is permitted but not required at any level.

6.4 Continuing Cyberspace Changes

Cyberspace continues to evolve technologically and globally. As a result, advanced techniques such as grid computing, distributed intelligent agent systems, distributed

knowledge management, and large-scale distributed systems of systems are being built without adequate protection mechanisms and will be susceptible to cyber attack. Additionally, within a few years, the largest makers of computer chips, the largest integrators of computers and network devices, and the largest producers of software will all be foreign software producers. This raises the level of anxiety about, if not the actual risk of, products containing hidden malicious functionality. Common Criteria evaluations, at present, do not provide sufficient screening to detect potential product behavior that is inconsistent with a product's intended use for high assurance systems [ENe-1].

6.5 Common Criteria Evaluation Costs

Common Criteria evaluations cost too much. This is especially true for low assurance products. Expectations of stakeholders, as discussed in Chapter 5, together with the high cost of evaluation often inhibit the use of appropriate small business and open source software [OCT-1, OCT-3]. The cost of evaluations is assumed to be insignificant (or at least not prohibitive) so that small businesses and independent developers, as well as large corporations, can have products evaluated. However, an evaluation may cost from as little as $30,000 to as much as $1,000,000 or more depending on a number of issues. This cost level for an evaluation may be a barrier to entry for open source software (OSS) and many products developed by small businesses [OCT-3]. As a result, many products may not be evaluated. By requiring use of evaluated products, Government policies eliminate products that may be more appropriate and sufficiently secure for the task. In interviews with small business stakeholders (see Chapter 5), they stated that evaluation costs are too high and they take too long [ECT-3, OCT-1, OCT-2]. Several interviewees believed that alternative assurance methods are needed, especially to reduce costs (such as a "CC lite") [EAa-3].

Relaxation of some of the documentation requirements at all levels is recommended. Documentation is expensive; the labs can determine when they have enough information of the right type.

6.6 Policy and Legal Landscape

The complexity of the cybersecurity policy landscape (see Chapter 3) and the confusion that complexity causes create problems in understanding. Policies are rapidly evolving, with both legislation and department and agency policies imposing new requirements and superseding each other. There is no single source for updated current policies, which makes it difficult for Government procurement offices to determine which requirements apply to their particular situation [FPCy-1].

6.7 Education, Training, and Awareness

Education, Training, and Awareness Programs have languished, are incomplete, and not current [FPEta-1, FPEta-2]. There is a critical need for education and training on several levels. IT product developers need a trained workforce to develop secure products. Developers are assumed to know about common mistakes (see Chapter 4) and how they lead to security vulnerabilities, and how to avoid those mistakes [AN-09].

Stakeholders expect the NIAP to require evaluators to demonstrate and maintain their technical competence [EPe-2, EPe-3]. In addition, stakeholders expect the NIAP to impose tighter constraints on evaluation labs when developing evidence for products the evaluation labs have under evaluation [EPe-1, EPe-4].

Finally, government IT system acquisition offices and system operators need a trained workforce to buy, implement, and maintain secure IT systems. As discussed in Chapter 5, consumers with only a basic familiarity of the NIAP processes often do not fully understand what an evaluation says about a product and are not able to determine whether a product meets their needs [EKn-3, OKn-1, OKn-2].

6.8 Flexible and Capably Staffed Program

NSA and NIST, without separate funding earmarked for the NIAP, have produced a flexible and capably staffed, although under-funded, product evaluation system [FN-1]. Moreover, it concluded that the shortcomings identified for the NIAP are addressable without a radical overhaul of the NIAP's product evaluation scheme. Revamping the administrative structure, processes, and expertise needed to create an alternate product evaluation scheme would be costly and time consuming, and there is little evidence that a more successful result would be achieved [RN-1].

6.9 Return on Investment

There is no return on investment (ROI) calculation for evaluated products. As Chapter 3 points out, the memorandum establishing the NIAP calls for research to develop objective measures of quality and security, but because of funding limitations, this research has not been conducted [FPRe-4]. A particular area of research that is being neglected is that of metrics to help consumers determine the ROI of evaluation. Stakeholders discussed in Chapter 5 reiterated that metrics that quantify both the security aspects of software and the effectiveness of evaluations are sorely lacking [ERe-1, ERe-2, ORe-1].

6.10 Maintenance Assurance and Flaw remediation

Common Criteria evaluations have not adapted to the development paradigm of release, patch, and update. Software producers often create new releases of products with defect corrections and minor functional enhancements. At present, the standard CC assurance packages for EAL1 through 7 have no provisions for accommodating such

minor changes. While maintenance assurance and flaw remediation packages are part of the standard, they are not part of any assurance packages. Deviations from the standard assurance packages are seldom made (a notable exception is that several NSA-developed PPs contain some of these provisions). Each new release may therefore be treated as a new product, requiring full evaluation. A number of stakeholders felt that analysis and testing of minor product changes, which would require considerably less effort than a full evaluation, should be sufficient to extend the original certificate to cover the updated product [EAM-1]. These provisions occur within the maintenance assurance packages. Further, it is expected that where security issues are involved, security failures and the patches to improve the product should be accompanied by notification to all registered users [EAM-2]. These provisions occur in the flaw remediation packages.

6.11 Evaluation Assurance

Evaluation assurance in the documented packages concentrates on documentation. The standard does allow for alternate assurance methods. The NIAP CCEVS, as documented in Chapter 4, requires no specific vulnerability analysis or testing methods that are releasable [FN-6]. Commercial software development practices differ widely and produce different documentation, as well as products with different types of defects. Requirements tracing through design and coding is assumed to be an effective security analysis technique, although there is little evidence that this contributes significantly to exposing security flaws.

Stakeholders interviewed in Chapter 5 agreed that the documentation required for evaluations is partly responsible for the high costs of evaluations [OCT-4]. While it is true that the CC do not require specific forms of documentation, they do spell out content required by assurance elements. Little of the documentation presented as evidence is part of normal development processes. This documentation is expensive to produce and often requires revision to satisfy evaluators.

6.12 Nefarious and Malicious Code

The current form of evaluation ignores the possibility of nefarious and malicious code. Product developers are assumed to be trustworthy and not knowingly insert malicious code into their products [AN-18, AN-19]. Stakeholders believe that malicious code and backdoor access paths inserted during development must be considered in any assurance arguments [ENe-1].

Although sources such as the *2001 Report of the Defense Science Board on Defensive Information Operations* note the need for research in scalable global computing, mobile code security, fault tolerance, and malicious code detection, they do not call for research to improve the CCEVS or the NIAP or for research in technologies directly related to them.

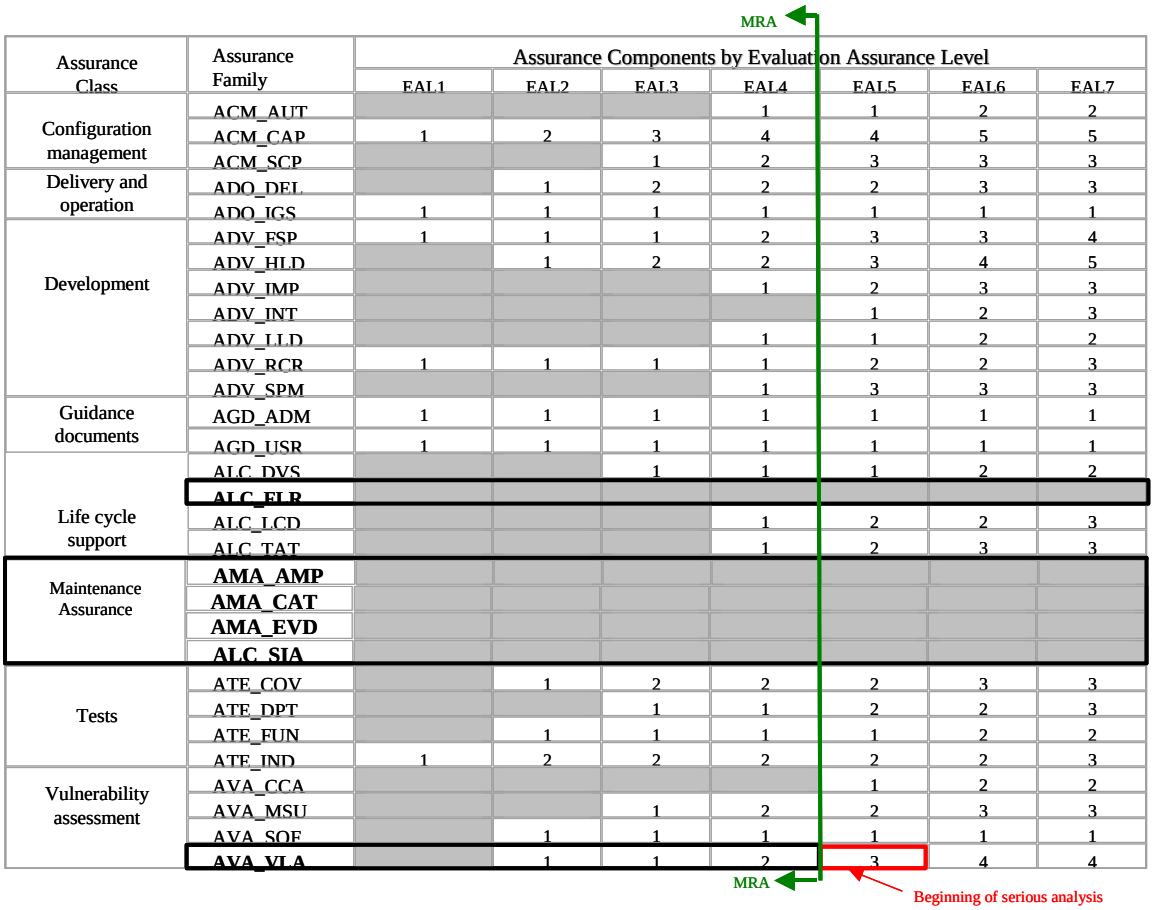
Although the detection of an arbitrary piece of malicious code is not currently solvable, tools can be developed to look for and discover certain types of more common malicious code. This would be of general benefit.

6.13 Common Criteria Issues

Several of the preceding sections dealt with adding work to evaluations when doing Common Criteria evaluations. Three areas in particular are worth further discussion: vulnerability testing, flaw remediation, and maintenance of assurance. All three are actually in the Common Criteria but not explicitly called out in assurance packages, or not at a high enough level (in the case of vulnerability work). Table 18 shows the Common Criteria assurance levels as taken from Part 3 of the Common Criteria standard. Assurance Maintenance, which is a standalone assurance class in the standard, has been added to the table. It should be specifically noted that Flaw Remediation (ALC_FLR) and Maintenance of Assurance packages (labeled as the Maintenance Assurance class in the table), are not included in any current assurance packages. Further, the stronger parts of the vulnerability analysis (AVA_VLA.3[22] and above) occur only at levels above those covered by the MRA. The latter is the subject of DoD protection profile additions to standard packages. The analysis team felt that these three should be included in all evaluations of IA and IA-enabled software.

[22] AVA_VLA3 is the third level of vulnerability analysis which in the table is not required until EAL5.

Table 18. Evaluation Assurance Level Summary



Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	2	2	2	3	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Maintenance Assurance	**AMA_AMP**							
	AMA_CAT							
	AMA_EVD							
	ALC_SIA							
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

6.14 Targets of Evaluation

The Target of Evolution (TOE) concept allows a developer to tailor the product that is being evaluated, which is often not the whole product or is some limited configuration of the product. While this is meant to tailor the evaluation to the IA aspects of the product and not cover the non-IA functionality, it is sometimes used to remove IA aspects (listed as optional, but not in the evaluated configuration) from evaluation. This is somewhat confusing to the consumers/acquirers of a product [ETOE-1]. Any feature of an evaluated product that can be accessed by the consumer/user should be part of the evaluation. Stakeholders expect whole products to be evaluated in their normal usage configuration and environment.

6.15 Conflicts and Compromise

It is clear that all expectations cannot be met. In fact several of the findings conflict with expectations, as well as expectations that conflict with expectations. Some examples follow.

6.15.1 Intellectual Property and the Need-to-Know

Market forces, which are discussed next, often dictate that a product may be differentiated by its unique intellectual property. For this reason controls are put in place to protect the intellectual property. There is a basic conflict between providing source code for analysis and protecting intellectual property that the code may reveal. A compromise might be to provide a standard set of code analysis tools to the code developer and allowing him to self-certify the results. Self-certification should only be used at low levels of assurance. Higher levels will require some form of verification. Another conflict is that between the evaluation laboratory processes that need protection and the need for system certifiers to see exactly what has been tested and the results of those tests. This has led to evaluation technical reports being unavailable. A compromise might be sanitized reports where applicable. Finally, the problem of developing effective metrics, tracking improvements, and tracking ROI is complicated by laboratory claims of proprietary cost methodology. Agreements should be worked out such that these data (metrics, tracking of improvements, and ROI) are made available for use in analyses while maintaining the proprietary aspects of the data generated by the laboratories.

6.15.2 Market Forces

The expectation for clear market viability [EMR-3] and some relation to reliability issues [OMR-1] leads to a conflict. Product evaluation will be performed, if available and cost effective, without mandate if it is in the best interest of the vendor. Market forces can make product evaluation a standard feature of development by reducing vendor costs and exposures (liability issues) or by providing product differentiation by increasing either market share or product worth. The consumer is the only one who can provide the market worth. Here education, training, and awareness are key.

> *Example 1.* For electrical products, consumers may refuse to buy a lamp for their home if it is not UL listed, and therefore, UL listing has worth to the producer of the lamp.

The cost, however, (discussed next) must be low enough that the increased market share or product worth allows recovery of the expenses. Consumers must know what an evaluated product provides over and above an unevaluated product, and this has not been adequately articulated. On the other hand, mandated evaluation, when favorable will be incorporated into vendor marketing.

> *Example 2.* For automobiles, a high EPA mileage rating is touted as a product differentiator.

The government must let the market do what it can and encourage market solutions. The market, however, sometimes needs help. When and where to mandate, and under what circumstances, involves sophisticated and subtle trade-offs.

6.15.3 Cost of Evaluation

The clear expectation is that evaluation costs should be reduced [OCT-1, ECT-1, ECT-2]. At the same time, it is also clear that stakeholders expect a more meaningful, technically detailed evaluation [ECm-1, EPP-2, ETe-2, ETe-3, etc.]. These latter sets of expectations drive up cost. The compromise is to provide enough assurance in the cybersecurity space to meet needs without adding unnecessary costs. There appears to be a split in the degree of assurance needed.

It is clear that for national security systems, defense critical applications, some banking transactions, and others, a high level of assurance is needed. In these systems the potential for loss is extremely high and probably worth the cost of a very thorough evaluation.

On the low assurance end, we suggest that product vendors (rather than products) be certified using a modification of processes like the SEI CMM. Under this approach, an annual or biennial evaluation would look at quality control, configuration control, flaw remediation, security processes, and maintenance assurance processes. This evaluation may cost $20,000 to $30,000 and can be done in a week. This certificate would ensure that a product was produced using the system, faithfully provides advertised functionalities (functional testing), and is relatively free from bad programming and known commonly exploited vulnerabilities (tools can help here). The emphasis would be on testing not documentation. Remarkably, this can be done under the Common Criteria, which allows the PP and ST to specify its own assurance verification processes. It is not clear that the Common Criteria Recognition Agreement would provide mutual recognition without some standardization of which evaluations are conducted and how.

On the high assurance end, the full Common Criteria approach is needed, with increased vulnerability testing (tools can help here), flaw remediation, and maintenance assurance packages added.

6.15.4 Compromise

While there are conflicts in needs, expectations, and implementation requirements, there are compromises that stem from the goals being pursued. The next two chapters review these options and provide a roadmap of phased-in compromise actions to generally raise cybersecurity awareness and overall system and product security.

7. Options

7.1 Introduction

A number of findings and recommendations have been presented in the previous chapters; however, simply addressing the individual problems illustrated will not solve the overarching concerns presented in Chapter 6. Moreover, two changes in the external environment have occurred. The first is a shift from government ownership and control of data to government ownership of data on civilian systems. The second is a shift away from government-owned systems upon which government decisions are based. There are seven environmental changes of note:

1. Change in systems ownership;
2. Change in data storage locations;
3. Change in computing and network capacity;
4. Change in user expertise;
5. Change to large, inter-connected government decision support systems;
6. Change in balance of static versus dynamic system composition toward dynamic system composition; and finally
7. Change in user demands and expectations of those systems.

Based on an analysis of the findings, recommendations, and areas of concern, IDA has identified six options for the NIAP, in increasing magnitude of change. The first three options do not respond to the changes in the external environment but present internal organizational changes to "improve the process." The next two options (Options 4 and 5) acknowledge that the environment external to the NIAP has changed significantly, and describe changes in the NIAP in response to that external environment, along with complementary internal changes. The final option (Option 6) not only acknowledges the changes in the external environment but also assumes that incremental changes in the process are an insufficient response and that a radical change in thinking, processes, and organization (or "transformation") is required.

Options 3, 4, and 5 build upon their predecessors and contain examples of the types of issues addressed by the option, with the arguments made both for and against. The set of activities within each option is not complete but is intended to give a general feel for the overall focus of the option. Decision makers may choose to implement only parts of the options, or one option plus portions of another. A roadmap for each of the options is presented in Chapter 8.

The final option could be executed in parallel with any one of Options 1 through 5. The options are as follows:

Option 1: Eliminate the NIAP;

Option 2: Continue the NIAP in its current form (reduced from the original intent);

Option 3: Restore the NIAP to the original intent of the Letter of Partnership between NSA and NIST;

Option 4: Modernize the approach to cybersecurity, but update the partnership to reflect changes in the environment since its creation in 1998;

Option 5: Take an integrated approach to cybersecurity; and

Option 6: Create a forward-looking approach to cybersecurity (new paradigm).

7.2 Descriptions of Options

The options below, with the exception of Option 1, are addressable within the current structure of the NIAP. Cost estimation was not done because of the large number of different implementations that can be undertaken. However Rough Order of Magnitude (ROM) values are as follows: Option 2 is double,[23] Option 3 is four times, Option 4 is six times, and Option 5 is eight times the current funding. Option 6 does not stand alone and is totally dependent upon which elements of its companion options are pushed into Option 6.

7.2.1 Option 1: Eliminate the NIAP

Description: With this option, the emphasis on product evaluation is shifted to C&A of systems. Separate efforts on software assurance are addressing the development of more secure software and applications from inception. This front-end effort would then become far more important, with the assumption that, if software and applications are developed in a more secure fashion, there would be a significantly reduced need to evaluate completed products. For those exceptional cases where additional assurance is needed, NSA would accomplish the required evaluations (as they do now), but the need for what are currently the EAL4 and below product evaluations would be removed. NIST would still continue to produce standards for the Federal community, as directed by FISMA, focusing on the C&A process and product and system configuration guidelines to ensure not only secure composition into a system but also secure operation within a Federal entity's IT infrastructure.

There are four versions of this option, all with different emphases:

1. Keep CCEVS, NSA takes the lead for DoD/NSS;

[23] To continue the NIAP in its current form, the funding must be increased to match the increase in the evaluation workload.

2. Eliminate product evaluation, drop out of CCEVS, focus on improving C&A;
3. Keep product evaluation, but do it another way (alternative forms of evaluation); and
4. Create a hybrid of versions 2 and 3, only specific evaluations done in an alternate form of evaluation or CC.

Pros: This is a relatively simple option to implement, since the requirements for C&A exist across the Federal Government and NIST is already addressing standards for C&A and configuration guidelines. Where product evaluation may still be required for those systems of highest sensitivity, NSA has the expertise and processes to do so for those activities (such as NSSs and the IC) requiring evaluations, and alternatives to the CCEVS are available to other Federal entities that wish to use them. This could also reduce the duplication of testing efforts between C&A and product evaluation and focus the efforts on C&A.

Cons: This option does not recognize any changes in the cybersecurity environment. It would most likely disqualify us from the MRA. DoD and NSS are still required to use evaluated products unless DoD and NSA are willing to change this requirement. It is unknown (has not been evaluated) whether the alternative evaluation methods are sufficient to address this need. This option puts significant additional emphasis on development of software assurance processes and methodologies that currently are not mature. It also puts the primary burden of cybersecurity on C&A processes and assumes that accreditors are knowledgeable enough and the processes are rigorous enough to ensure that the process results in a secure system ready to operate. If the version of this option is to not do product evaluations at all, it could be seen as turning our back on evaluations and stating that the labs are not commercially viable – a loss of investment on the part of the labs.

7.2.2 Option 2: Continue the NIAP in its Current Form

Description: With this option, the NIAP would continue to be a partnership between NIST and NSA, but it would continue to almost exclusively monitor product evaluations and interact with the MRA partners on improvements to the Common Criteria. More personnel would be needed to handle the growth of evaluations. The complex legal and guidance issues could be clarified by the use of a legal clearinghouse (see Chapter 3 for a discussion of statutory and policy requirements). This clearinghouse would clearly be over and above the previous NIAP functionality, as are many others we will suggest.

Pros: Because this is a continuation of the current state, there are no obstacles to overcome, so this option presents the lowest technical risk. Any other needs will have to be met by the development of new processes/practices outside of the NIAP/CCEVS.

Cons: Budget issues would have to be resolved through the agencies. Like Option 1, this option ignores or does not respond to the significant changes in the cybersecurity environment. What the NIAP does and how the responsibilities are assigned within the partnership depend on the current budgets and spending priorities of the partners. Without making significant interfaces to C&A, much of what can be accomplished with product evaluation may not be reused and in that sense can be viewed as a duplicative or wasteful effort. Leaving the NIAP in its current reduced state of operations satisfies only the formality of having an evaluation process to replace the Orange Book (CSC-STD-001-83, Trusted Computer System Evaluation Criteria, National Computer Security Center (NCSC)) evaluations of the past. To continue the NIAP in the current form, the funding must be increased to match the increase in evaluation workload.

7.2.3 Option 3: Restore NIAP

Description: This option restores the NIAP to the full functioning envisioned when the partnership was first established in 1998, without regard to the changes in the environment that have occurred since its inception. The partnership between NIST and NSA would be formalized in some way (more formally than the existing Letter of Partnership between the parties), with the responsibilities of each party spelled out in detail, i.e., NIST certifies evaluation laboratories, provides a full-time person to work with commercial sectors (finance, health care, telecommunications, etc.) to specify their security requirements, and participates in the CC. NSA would be required to provide enough validators to adequately oversee validations done by the labs, handle validations above EAL4, and participate in the CC. Funding will be a real issue, since NIST and NSA have not agreed to fund the NIAP at these levels in the past.

The original vision was that the NIAP would produce tools, provide education about the CC, and write security specifications. Also part of its original scope (see Section 1.2) was to "Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics."[24] Part of the original scope was the development of PPs beyond the DoD to other Government departments, critical infrastructure, and private sectors as the tasking has or should evolve to provide education, including on writing PPs and STs and interpreting evaluation certificates. These functions would now be performed as originally intended.

Pros: The primary focus of this option is the restoration of the NIAP to its original mission and a formal recognition of this mission. This option would clarify duties and responsibilities of the parent organizations, set out detailed requirements, and provide for oversight mechanisms. The analysis tools would lead to better testing at a lower cost. The

[24] Letter of Partnership National Security Agency and National Institute of Standards and Technology, August 22, 1997.

development of tools for automating the simpler aspects of security evaluation could raise the security level of all evaluated products. The NIAP would also perform other critical functions required to make product evaluation both understandable and useful, as well as the product evaluation core function.

Cons: Budget requirements would have to be resolved through the agencies (NSA and NIST), and they have not been able to agree to full funding for this option in any year except the first – shortly after the memorandum of agreement was signed. Additional funding may have to be provided to NIST and NSA. As with Options 1 and 2, this option does not address any changes indicated by the current environment. This option also does not address the issue of how the product evaluation fits into the C&A process, which makes little use of product evaluations and duplicates some of the effort and cost of the product evaluations, especially where these product characteristics implement system-level controls. This option also does not address how product evaluations fit in the overall Federal cybersecurity effort. Because it does not address some of the fundamental concerns about the product evaluation process – although this may be a desirable option to address short-term issues – in the long run, it may not be a justifiable expenditure of scarce resources.

7.2.4 Option 4: Modernistic Approach to Cybersecurity

Description: With this option, the original charter of the NIAP is restored but updated to address changes in the environment, including its relationship to C&A and the Federal cybersecurity program. Since most unintentional vulnerabilities are caused by a relatively small set of common implementation errors, and many of these errors can be detected or countered by tools, employing various tools should improve the cost-effectiveness of the evaluation process in general. This update provides for a formalization of the NIAP as an entity with a more stable funding source, separate from the agency budgets, and providing a detailed set of requirements together with oversight. The evaluators conducting C&A processes would be more than happy to take advantage of product evaluation data, which must be made available to C&A accreditors. To the extent that the administrators of NIAP/CCEVS can change their documentation and evidence to also meet the needs of system security certification agents (and system auditors, system developers/integrators), these evaluation deliverables may prove useful. This option would include vulnerability testing in all evaluations and the development in test methods in conjunction with PP development and evaluation work units.

Additional responsibilities in this new environment would include a more aggressive partnership with industry to ensure the cost-effectiveness of this effort, and an aggressive, coherent ET&A effort. This option could institute a number of improvements to the evaluations identified as current shortfalls. New assurance techniques (peer review, source code review tools, etc.) would be evaluated and added to PPs and evaluation

schemes. The modernized NIAP would work to incorporate these techniques into the CC. Personnel in laboratories and government would undergo a credentialing program.

Pros: This option directly addresses changes in the cybersecurity environment that have occurred since the NIAP was established, including the new requirements of FISMA and challenges posed by foreign software development and foreign chip development, by requiring the use of tools that will examine these issues (such as nefarious code development). The ET&A would ensure an educated consumer who is identified as a critical concern. Maintenance assurance and flaw remediation programs would maintain product security through the normal software development cycles. Increased and improved testing would cover some aspects of the concerns for screening against nefarious or malicious code. It also provides a more cost-effective process, encouraging industry participation.

Cons: Budget requirements would have to be resolved through the agencies. Although this option does acknowledge and address changes in the cybersecurity environment (Federal, state/local, and private sector), it requires policy, responsibility, and programmatic changes in an already complicated situation. It may also require some changes to ET&A programs outside of the NIAP (DITSCAP, etc.). Additional research and development would be required to implement this option.

7.2.5 Option 5: Integrated Approach to Cybersecurity

Description: This Option looks at a state beyond the current thinking of what the NIAP was originally intended to be and addresses the larger issue of what an integrated approach should be to ensure secure, functional information processes for the Federal Government as IT continues to evolve into new areas. It is a logical extension of the NIAP's charter to look at not only product evaluation from the end-point but at software assurance in developing more secure and reliable products and then ensuring the proper configuration and operation of that product in a systems environment. Some of the issues to be addressed in this option include: advice and consent for products in the C&A process and development of more comprehensive and robust configuration guidelines. There is no guarantee that user organizations can/will adhere to the evaluation environments/configurations. However, even if evaluated products are not used in their evaluated environment/configuration, C&A must be performed. It is unreasonable to expect the evaluated configuration to meet the needs of all users of a product. C&A is performed independently of whether an evaluated product is used in a system and is independent of whether the product is used in its evaluated configuration. Using evaluated products in a system should not be construed as forcing the system developers to implement the system in the evaluated configurations. In fact, when using several evaluated products in a system, it is highly unlikely that the configuration requirements of each product can be met simultaneously. The advice and consent will assist in evaluating

the impact of these configuration and environment changes. This option would also address the NIAP participation in increased and focused research into areas directly contributing to this effort.

Pros: This option acknowledges that the environment has changed since the original NIAP charter and addresses changes required by that new environment. It would recognize assurance techniques that are not yet incorporated into the CC, while at the same time maintaining international mutual recognition where possible. The ET&A would ensure an educated consumer who is identified as a critical concern. Maintenance assurance and flaw remediation programs would maintain product security through the normal software development cycles. Increased and improved testing would cover some aspects of the concerns for screening against nefarious or malicious code. It also provides a more cost-effective process, encouraging industry participation.

Cons: Budget requirements would have to be resolved through the agencies. This option may require significant changes in policy and practice outside of the NIAP itself that may present overwhelming challenges to existing organizations unless their responsibilities are re-scoped. Using additional assurance techniques requires evaluating how these techniques interact with the techniques already in use. Training would have to be provided to the evaluation laboratories. Changes to the CC would require international consensus and may take time. Automated source code review may be a tricky issue with respect to intellectual property rights. Vulnerability testing and source code review would be greatly facilitated by tool development. It may also require some changes to ET&A programs outside of the NIAP (DITSCAP, etc.). Additional research and development would be required to implement this option.

7.2.6 Option 6: Forward Looking Approach to Cybersecurity (new paradigm)

Description: The sixth option is to move the approach to security evaluation to a new paradigm for operation and evaluation that would better address the wide-ranging changes that have occurred in the environment and community that the NIAP must serve. This is not a change in the NIAP following the progression already described, but a whole new way of thinking about the problem of cybersecurity. While it is not possible to describe this option and associated resource requirements in actionable detail without further study, several aspects of this option are clear at this time.

The new paradigm must address, in a holistic manner, the risks to and vulnerabilities of systems. It must ensure that the security of a system is greater than that of the sum of its parts. It must also address issues related to changes in system ownership, rapid changes in system composition, changes in data ownership and location, changes in user expertise, and increasingly complex systems. In other words, the new paradigm must be as dynamic as the environment within which it must work.

Clearly, there are many approaches for specifying and assessing security functionality other than using the critical criteria. For example, the open source approach of having many independent observers perform code reviews would perhaps ease fears of trap doors and Trojan horses. Alternatively, evaluators could observe a product producer's methodology, in lieu of assessing documentation. Other schemes may include active lab vulnerability testing for all new identified vulnerability threats (viruses, Trojan horses, etc.). The NIAP is not currently disposed to require these types of tests, although they have considered it and even drafted (but not approved) some policy in this area.

Pros: This option acknowledges that, even with changes that address the current environment, innovative thinking will be required to keep ahead of the threats and vulnerabilities in cybersecurity. Adoption of this option would ensure that cybersecurity evaluations remain relevant in a dynamic environment.

Cons: This option does not solve the near-term problems with the NIAP, so it must be pursued in combination with the other options described above. There is also technical risk with this option since nothing in the current Defense Advanced Research Projects Agency (DARPA) or NSF research pipelines is addressing a new paradigm.[25]

7.3 Examining the Options in the Performance/Cost Trade Space

The key to providing performance/cost trade space options is in having good data. We have seen, however, that a metrics program was never put in place. There are no performance statistics to say how well the cybersecurity approaches are doing in general, and with and without product evaluation under the current process. Nor is there accurate cost data because of the commercial laboratory system and because of costs and budgets being treated as proprietary data. The first priority in any of the options that seek to improve performance is to do the research necessary to establish metrics (including costs) and to put a metrics program in place. Further, as delineated in Option 6, an annual report and an independent assessment should be provided until there is enough data to properly

---

[25] In testimony to the U.S. House of Representatives Committee on Science in May 2003, DARPA Director Dr. Tony Tether described DARPA's past investments in information assurance and cybersecurity research. This work included development and improvement of firewalls, intrusion detection methods, and intrusion tolerance techniques that allow systems to operate through attacks. The bulk of this research, from DARPA's point of view, has been completed and DARPA has moved on to more advanced concepts of cognitive computing in which computer systems are expected to know what they are doing – including knowing when they are under attack and how to respond. DARPA's original firewall research has matured into widely used commercial products. The remainder of this research is still in the proof of concept and product development pipeline.

Also in 2003, NSF started a process to reinvigorate their Cyber Trust program. In 2004, NSF funded 50 research projects addressing different aspects of computer and network security, privacy, and trust. Virtually all of this research focuses on fundamental research questions that have long-range implications. This work, however, is not intended to address today's immediate computer security problems. Research results that can be transitioned quickly into products and applications are good, but this is not a criterion NSF uses in selecting research projects for funding.

understand how the actions needed to achieve the various options provide the trade-off between cost and performance. These analyses should be part of the near-term efforts and be completed before proceeding to mid-term efforts. Once metrics exist, thresholds and requirements can be derived. This directly applies to Options 3 through 6. Nonetheless, a notional representation of that trade space is presented in Figure 7. This notional representation was developed by the analysts to illustrate how these changes may affect the performance/cost trade space. In this figure, rough estimates based upon experience and a little analysis are presented to provide a "feel" for the options outlined in this chapter and presented in detail in the next chapter. The data is unreliable, and the metrics program should be the first indication of its correctness in terms of trend.

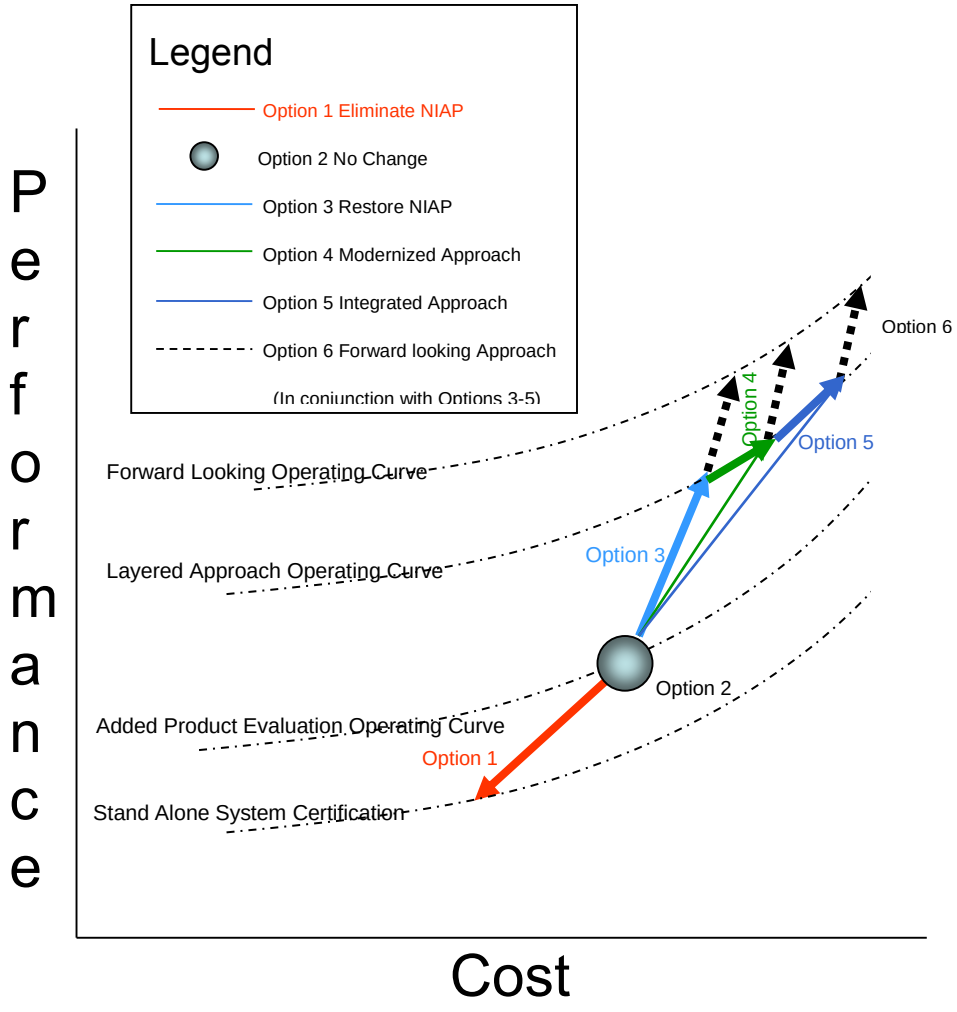


Figure 7. Notional Performance/Cost Trade Space for the Six Options Presented

7.4 Summary

This chapter has attempted to provide a series of options that address the issues raised in previous chapters and how those issues might be addressed, from maintaining the status quo to the most radical new thinking. What is apparent from the analysis presented in the prior chapters is a feeling in the community at large that the status quo (Option 2) is not meeting expectations and that something must change. Whether the change is to discontinue requiring product evaluations for the lower assurance levels or improve the process, consideration must be given to the changes required in policy, processes, and resources so that an informed decision, with an understanding of the costs and benefits and ultimate consequences, may be made. The areas where expectations are not met can generally be improved with an increased emphasis (e.g., funding) or a new requirement for evaluation. Many expectations are conflicting and cannot all be met. It is also noted that the Government is not responsible for meeting all of the cyberspace requirements, but it should place a structure in place that raises the level for all concerned without undue burden on any sector. Chapter 8 builds on these options by providing a roadmap for improving the NIAP.

8. Roadmaps for Accomplishing Options

The preceding chapters have provided recommendations and options without context. They have indicated individual discrepancies in the current system with an indication of what is needed to repair them. Reference tags are used when findings and recommendations would otherwise be repeated. After each action to be undertaken for an option are tags to related findings or recommendations.

The purpose of this chapter is to provide a coherent approach for implementing each of the options. It should be noted that many of the actions in the options are beyond the functionality that the NIAP was originally intended to undertake. Indeed many may be outside of NIAP control and require input or actions from other agencies or legislative action.

8.1 Option Roll-out

Options 2 through 5 form a set of increasing requirements. As such, exercise of the option elements can fit budgetary constraints initially; however, longer-term commitments are made as the option number increases. The options and their relationships to each other are shown in Table 19 below.

Table 19. Relationships of the Various Options

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
1	Eliminate NIAP	8.2	Elimination		
2	Continue Current NIAP	8.3	1. Trained Personnel. 2. Requirements. 3. Security Support Group. 4. ISO/CC. Cost Reduction. Standards.		
3	Restore NIAP	8.4	1. Option 2+ 2. Requirements.+	1. C&A Interface. 2. NIAP Process Improvement.	
4	Modernized Approach to Cybersecurity	8.5	1. Option 3+ 2. Formalization. 3. Testing. 4. Security Support Group. + 5. NIAP Process Improvement.	1. Option 3+ 2. C&A Interface. + 3. NIAP Process Improvement. + 4. ISO/CC. Cost Reduction. Standards. 5. Consolidation. 6. Security Support Group.	1. Cost Reduction. 2. Consolidation. 3. ISO/CC. Cost Reduction. Standards.

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
5	Integrated Approach to Cybersecurity	8.6	Option 4	1. Option 4 + 2. C&A Interface. +	Option 4
6	Forward-looking Approach to Cybersecurity	8.7	Independent Assessment		Independent Assessment

In an ideal world, budgets would allow us to do through Option 4, which represents a modernization of the NIAP process to fit the world changes that have evolved since its inception. Option 5 adds to this, but no significant additions exist until the mid-term, allowing a rollout and evaluation of Options 4 and 5 until the mid-term, at which point a choice can be made. Option 6 should be implemented in any event because it will monitor and provide updates and coordination of cybersecurity issues.

8.2 Option 1: Eliminate the NIAP

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
1	Eliminate NIAP	8.2	Elimination		

Eliminating the NIAP is not recommended [FN-1, RN-1]. It is recommended that the NIAP, as an entity, be retained. The NIAP has many shortcomings that need to be addressed, but its strength is in the gathering of expertise, the development of an infrastructure, and its programmatic ties to the international community. While a new organization or approach could be developed, the administrative burden of recreating these strengths is large and without guarantee of greater success. Having said that the NIAP should be retained, it is recommended that it immediately be strengthened and improved and moved toward a process that is more responsive to stakeholders and the nation's needs and that fits better within the architecture of software assurance processes.

Options 2 through 5 assume that a properly developed and integrated product evaluation is necessary to an overall program of cybersecurity. This overall program includes specific algorithm evaluations overseen by NIST (as in FIP-140) and system-level evaluations as prescribed in DITSCAP, NIACAP, and OMB/FISMA.

8.3 Option 2: Continue the NIAP (in its current form)

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
2	Continue Current NIAP	8.3	1. Trained Personnel. 2. Requirements. 3. Security Support Group. 4. ISO/CC. Cost Reduction. Standards.		

If Option 2 is undertaken, then the following actions need to be taken as quickly as possible:

2-1 near-term. **Trained Personnel.** Establish a program to increase the number of educated, trained evaluation personnel. [RPEta-1, FN-2, AN-22, FEPe-1, ES-06]

2-2 near-term. **Requirements.** Include some NIST participation, and adequate resources for the evaluation function. [RPCy-2, FPCy-2, RPCy-3, ENi-1, ENi-2]

2-3 near-term. **Security Support Group.** Set up a security support group (SSG) to provide legal/guidance and policy consolidation services (legal clearinghouse activities). [FPCy-1, RPCy-1]

2-4 near-term. **ISO/CC. Cost Reduction. Standards**. Push ISO/CC to accept vendor documentation in lieu of CC-developed evidence (cost reduction). [AN-11, OCT-1, OCT-2]

8.4 Option 3: The NIAP Restored to the Original Intent

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
3	Restore the NIAP	8.4	1. Option 2+ 2. Requirements.+	1. C&A Interface. 2. NIAP Process Improvement.	

If Option 3 is undertaken, then the following actions should be taken as quickly as possible:

3-1 near term. **Trained Personnel.** Establish a program to increase the number of educated, trained evaluation personnel. [AN-22, RPEta-1, FN-2, FEPe-1, ES-06]

3-2 near term. ***Requirements.***[26]

1. *Include a fully participating NIST*[27] *and potential new partners such as DHS. Other potential new partners such as Consortia and academia would provide their own funding.* [RPSt-1]
2. *Funding should be applied to research, metrics (including ROI metrics), tool development (source code scanners, port sniffers, test benches for specific vulnerabilities, etc. – not on tools to help document evaluation).* [RPCy-3, FPRe-1, FPRe-5, RPRe-2, FN-2, FERe-1, ES-12]
3. *Metrics should be tracked and analyzed, at least annually until a clear picture of the worth of other actions may be perceived.*
4. *Development and dissemination of training materials for developers, managers, users, consumers, and others not involved in the evaluation process.* [FN-6, FPEta-11, FPEta-2, RPEta-1, FEKn-2, AN-17, ES-01]
5. *CC Standards participation and PP development as well as evaluations.* [FEPP-1, RN-1, ES-04, ES-05]
   (finish mid-term, start near-term).[28]

[26] Text in *italics* indicates new actions not found in lower numbered options.
[27] In all aspects of NIAP, including research, tools, education and CCEVS as well as NVLAP.

3-3 near term. **Security Support Group.** Set up a security support group (SSG) to provide legal/guidance and policy consolidation services (legal clearinghouse activities). [FPCy-1, RPCy-1]

3-4 near term. **ISO/CC. Cost Reduction. Standards**. Push ISO/CC to accept vendor documentation in lieu of CC-developed evidence (cost reduction). [AN-11, OCT-1, OCT-4]

If Option 3 is undertaken, then these items should be begun as soon as they can be practicably started:

3-1 mid-term. ***C&A Interface.*** *Make evaluation technical reports and testing data releasable to C&A authorities.* [RPAq-3, FECa-1]

3-2 mid-term. ***Improvement of the NIAP Processes.*** *Develop publicly available tools, a NIST web site for distribution and maintenance, and tasking to keep up to date.* [AN-08, FETe-1]

8.5 Option 4: Modernized Approach to Cybersecurity

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
4	Modernized Approach to Cybersecurity	8.5	1. Option 3+ 2. Formalization. 3. Testing. 4. Security Support Group. + 5. ISOKC+ 6. NIAP Process Improvement.	1. Option 3+ 2. C&A Interface. + 3. NIAP Process Improvement. + 4. ISO/CC. Cost Reduction. Standards. 5. Consolidation. 6. Security Support Group.	1. Cost Reduction. 2. Consolidation. 3. ISO/CC. Cost Reduction. Standards.

If Option 4 is undertaken, then the following items should be done as quickly as possible:

4-1 near-term. **Trained Personnel.** Establish a program to increase the number of educated, trained evaluation personnel. [AN-22, RPEta-1, FN-2, FEPe-1, ES-06]

4-2 near-term. ***Formalization.*** *Immediately formalize the NIAP by providing a funding line and specific requirements associated with its intended purposes*. [RPCy-2]

4-3 near-term. **Requirements.**

1. Include a fully participating NIST and potential new partners such as DHS. Other potential new partners such as Consortia and academia would provide their own funding. [RPSt-1]
2. Funding should be applied to research, metrics (including ROI metrics), tool development (source code scanners, port sniffers, test benches for specific vulnerabilities, etc. – not on tools to help document evaluation). [RPCy-3, FPRe-1, FPRe-5, RPRe-2, FN-2, FERe-1, ES-12]

[28] Additional requirements from previous options are shown in italics.

3. Metrics should be tracked and analyzed, at least annually until a clear picture of the worth of other actions may be perceived. [FN-6, FPEta-11, FPEta-2, RPEta-1, FEKn-2, AN-17, ES-01]
4. Development and dissemination of training materials for developers, managers, users, consumers, and others not involved in the evaluation process. [FN-6, FPEta-11, FPEta-2, RPEta-1, FEKn-2, AN-17, ES-01]
5. CC Standards participation and PP development as well as evaluations. [FEPP-1, RN-1, ES-04, ES-05]
(finish mid-term, start near-term).

4-4 near-term. **Testing.** Require **all** evaluations to undergo vulnerability analysis, testing as well as assurance maintenance and flaw remediation (the *latter two are not now a requirement in any assurance packages*[29]*, and little specific application of testing and vulnerability analysis are required at EAL4 and below).* [AN-07, FN-6, FETe-3, FEAM-1]

4-5 near-term. **Security Support Group.** Set up a security support group (SSG) to provide legal/guidance and policy consolidation services (legal clearinghouse activities). *The SSG will also provide analysis of cybersecurity research in government, industry, and academia*. [FPCy-1, RPCy-4, FPRe-2, FPRe-3]

4-6 near-term. **ISO/CC. Standards**. *Push ISO/CC to include test in CEM and PPs*. Push ISO/CC to reduce evaluation paperwork requirements. [FETe-2, AN-11, OCT-1, OCT-4]

4-7 near-term. ***Improvement of the NIAP Processes.*** *Develop a personnel certification process and credential all evaluators and validators (finish mid-term, start near-term).* [AN-22, FEPe-1]

If Option 4 is undertaken, then these items should be begun as soon as they can be practicably started:

4-1 mid-term. **C&A Interface.** Make evaluation technical reports and testing data releasable to C&A authorities. [RPAq-3, FECa-1]

4-2 mid-term. ***C&A Interface.*** *Modify C&A under OMB, DITSCAP, NIACAP, etc., to allow reuse of the product evaluation data.* [FPAq-2, RPAq-3]

4-3 mid-term. **Improvement of the NIAP Processes.** Develop publicly available tools, a NIST web site for distribution and maintenance, and tasking to keep up to date. Require that tools be run against all evaluated products. [AN-08, FETe-1]

4-4 mid-term. ***Improvement of the NIAP Processes.*** *Develop a personnel certification process and credential all evaluators and validators (finish mid-term, start near-term).* [AN-22, FEPe-1, ES-06]

---

[29] DoD may be addressing each of these as cited previously in the text, but a more formal and wider application is needed for DHS considerations. (see section 8.8)

4-5 mid-term. ***ISO/CC. Cost Reduction. Standards****. Push ISO/CC to require the use of tools for all evaluated products.* [AN-07, AN-09, RN-1, FETe-2, FETe-3]

4-6 mid-term. ***Consolidation.*** *Bring all of Federal Government under the product evaluation mandate similar to NSTISSIP (but not until tools are available and a stable set of PPs are developed at all levels). – Legislative and policy issues.* [FPSt-2, FPAq-1, RPAq-1, RPAq-2]

4-7 mid-term. ***Security Support Group.*** *Institute ROI studies by the SSG, using the metrics developed under near-term 4-3.* [FPRe-4, FPRe-5, RPRe-2, AN-16, AN-23]

4-8 mid-term. Adjust based on mid-term 4-7.

If Option 4 is undertaken, then these items are follow-on and should be started at appropriate times as indicated by completion of other items on the lists above:

4-1 long-term. ***Cost Reduction.*** *After item mid-term 4-3 is complete, set up an alternate assurance process for products of basic security that includes only the tools, security function verification, and vendor process evaluation (goal – cost effective evaluations that raise the bar for everyone). Equivalent EAL3-4 and above to be done through Common Criteria.* [EAa-1, OAa-1]

4-2 long-term. ***Consolidation.*** *Include critical infrastructure under this mandate. – Legislative and policy issues need to be resolved.* [ECI-1, ECI-2, ECI-3, OCI-1] *Include selected product classes outside of the normal IA or IA-enabled product type.* [AN-27]

4-3 long-term. ***ISO/CC. Cost Reduction. Standards****. Push CC to this level (described in 4-1 long-term).* [AN-20]

8.6 Option 5: Integrated Approach to Cybersecurity

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
5	Integrated Approach to Cybersecurity	8.6	Option 4	1. Option 4 + 2. C&A Interface. +	Option 4

If Option 5 is undertaken, then the following items should be done as quickly as possible:

5-1 near-term. **Trained Personnel.** Establish a program to increase the number of educated, trained evaluation personnel. [AN-22, RPEta-1, FN-2, FEPe-1, ES-06]

5-2 near-term. **Formalization.** Immediately formalize the NIAP by providing a funding line and specific requirements associated with its intended purposes. [RPCy-2]

5-3 near-term. **Requirements.**

1. Include a fully participating NIST and potential new partners such as DHS. Other potential new partners such as Consortia and academia would provide their own funding. [RPSt-1]
2. Funding should be applied to research, metrics (including ROI metrics), tool development (source code scanners, port sniffers,

test benches for specific vulnerabilities, etc. – not on tools to help document evaluation). [RPCy-3, FPRe-1, FPRe-5, RPRe-2, FN-2, FERe-1, ES-12]

3. Metrics should be tracked and analyzed, at least annually until a clear picture of the worth of other actions may be perceived. [FN-6, FPEta-11, FPEta-2, RPEta-1, FEKn-2, AN-17, ES-01]
4. NIAP-funded evaluations for small business and open source software where the developers cannot fund the evaluation (possibly requiring free/low-cost use/support, modification rights, and/or specialized changes). [OCT-8, ECT-1, ECT-2]
5. Development and dissemination of training materials for developers, managers, users, consumers and others not involved in the evaluation process. [FN-6, FPEta-11, FPEta-2, RPEta-1, FEKn-2, AN-17, ES-01]
6. CC Standards participation and PP development as well as evaluations. [FEPP-1, RN-1, ES-04, ES-05]
(finish mid-term, start near-term).

5-4 near-term. **Testing.** Require **all** evaluations to undergo vulnerability analysis, testing as well as assurance maintenance and flaw remediation (the latter two are not now a requirement in any assurance packages, and little specific application of testing and vulnerability analysis are required at EAL4 and below). [AN-07, FN-6, FETe-3, FEAM-1]

5-5 near-term. **Security Support Group.** Set up a security support group (SSG) to provide legal/guidance and policy consolidation services (legal clearinghouse activities). The SSG will also provide analysis of cybersecurity research in government, industry, and academia. [FPCy-1, RPCy-4, FPRe-2, FPRe-3]

5-6 near-term. **ISO/CC. Cost Reduction. Standards**. Push ISO/CC to include test in CEM and PPs. Push ISO/CC to reduce evaluation paperwork requirements. [FETe-2, AN-11, OCT-1, OCT-4]

5-7 near-term. **Improvement of the NIAP Processes.** Develop a personnel certification process and credential all evaluators and validators (finish mid-term, start near-term). [AN-22, FEPe-1]

If Option 5 is undertaken, then these items should be begun as soon as they can be practicably started:

5-1 mid-term. **C&A Interface.** Make evaluation technical reports and testing data releasable to C&A authorities. [RPAq-3, FECa-1

5-2 mid-term. ***C&A Interface.*** *Institute a program of advice and consent, where the NIAP participates in C&A and advises on the use, configuration, and environment for evaluated products, as well as other functions as delineated in Chapter 6.* [FPAq-2, RPAq-3]

5-3 mid-term. **C&A Interface.** Modify C&A under OMB, DITSCAP, NIACAP, etc., to allow reuse of the product evaluation data, *and recommend the NIAP Advise and Consent of element 2.* [FPAq-2, RPAq-3]

5-4 mid-term. **Improvement of the NIAP Processes.** Develop publicly available tools, a NIST web site for distribution and maintenance, and tasking to keep up to date. Require that tools be run against all evaluated products. [AN-08, FETe-1]

5-5 mid-term. **Improvement of the NIAP Processes.** Develop a personnel certification process and credential all evaluators and validators (finish mid-term, start near-term). [AN-22, FEPe-1, ES-06]

5-6 mid-term. **ISO/CC. Standards**. Push ISO/CC to require tools run against all evaluated products. [AN-07, AN-09, RN-1, FETe-2, FETe-3]

5-7 mid-term. **Consolidation.** Bring all of Federal Government under the product evaluation mandate similar to NSTISSIP (but not until tools are available and a stable set of PPs are developed at all levels). – Legislative and policy issues. [FPSt-2, FPAq-1, RPAq-1, RPAq-2

5-8 mid-term. **Security Support Group.** Institute ROI studies using the metrics developed under near-term 5-3. [FPRe-4, FPRe-5, RPRe-2, AN-16, AN-23]

5-9 mid-term. Adjust based on mid-term 5-8.

If Option 5 is undertaken, then these items are follow-on and should be started at appropriate times as indicated by completion of other items on the lists above:

5-1 long-term. **Cost Reduction.** After mid-term 5-3 is complete, set up an alternate assurance process for products of basic security that includes only the tools, security function verification, and vendor process evaluation (goal – cost effective evaluations that raise the bar for everyone). Equivalent EAL3-4 and above to be done through Common Criteria. [EAa-1, OAa-1]

5-2 long-term. **Consolidation.** Include critical infrastructure under this mandate. – Legislative and policy issues need to be resolved. Include selected product classes outside of the normal IA or IA-enabled product type. [AN-27]

5-3 long-term. **ISO/CC. Cost Reduction. Standards**. Push CC to this level (described in long-term 5-1). [AN-20]

8.7 Option 6: Forward looking Approach to Cybersecurity

Option	Title	Details	Actions Required		
			Near-term	Mid-term	Long-Term
6	Forward looking Approach to Cybersecurity	8.7	Independent Assessment		Independent Assessment

Option 6 does not stand alone, because it does not have an immediate process for replacing Options 3 through 5. However, Option 6 does not apply nor should it be used in conjunction with Options 1 or 2. If Option 6 is undertaken, then the following items should be done as quickly as possible:

6-1 near-term. ***Instantiate*** *one of Options 3-5 in the interim.*

6-2 near-term. ***Independent Assessment.*** *Provide independent and periodic audits of the cybersecurity process. This should include tabulation and analysis of the metrics developed under the option chosen.*

6-3 near-term. ***Independent Assessment.*** *Provide for an annual report for the state of nation's cyberspace security.*

6-4 near-term. ***Security Support Group. Standards****. Augment the CC interface with related standards works.*

If Option 6 is undertaken, then these items are follow-on and should be started at appropriate times indicated by completion of other items on the lists above:

6-1 long-term. ***Independent Assessment.*** *Provide for the overall coordination of the cyberspace activities and provide an arbitrage service where the needs of various elements (i.e., C&A and or product evaluation) come into conflict.*

Independent Assessment. *Institute new approaches as reported by the above.*

8.8 Amplifying Comments for specific action items.

8.8.1 Trained Personnel

The need for trained personnel is an underlying problem that must be addressed for any of the viable options. As described in Chapter 4, the NIAP relies upon a core group of highly educated, trained, and experienced experts in both cybersecurity evaluation and standardization. The growth of the IT applications in general, combined with increased connectivity and complexity of security issues, will overwhelm this core group. As it is, the NIAP is barely keeping up with evaluations.

The personnel shortage will not be solved in the near term, but it will never be solved if a program is not undertaken to increase the expertise pool. The degree to which this shortage of trained personnel affects operations increases in severity as Options 2 through 5 are considered. As the notional estimates in Figure 8 illustrate, Options 2 through 5 require increasing numbers of not only people but also processes and technologies. Requirements for Option 6 are in addition to those of the other option selected, with the exception of Option 5, from which the Independent Assessment in Option 6 picks up several of the requirements. Additionally, the alternative assurance methods for basic security software described in Options 4 and 5 may reduce overall resource requirements.

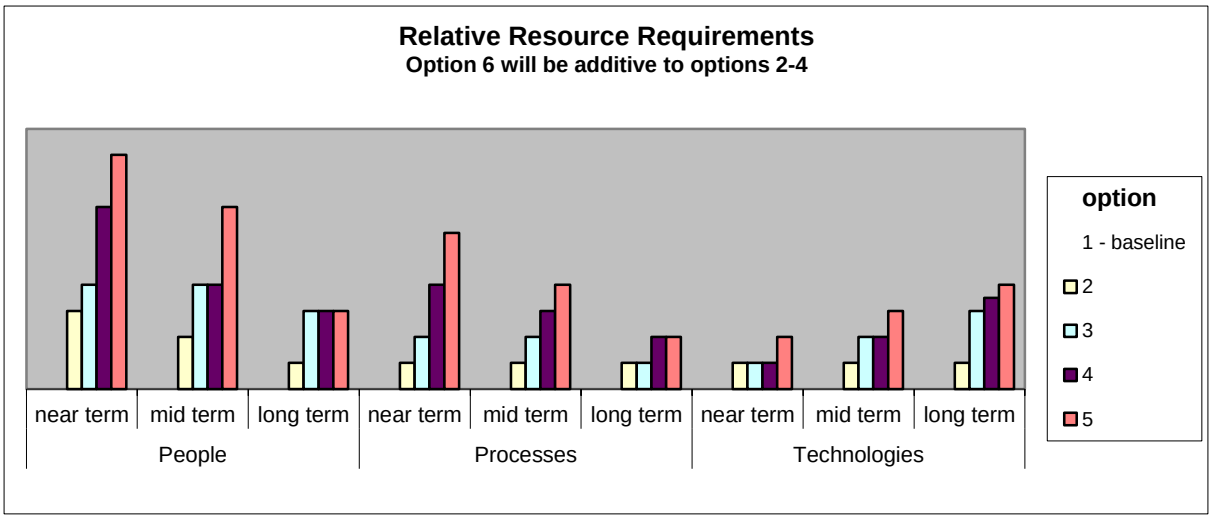


Figure 8. Rough Order of Magnitude (ROM) Resource Requirement

8.8.2 Requirements

Safeguarding cyberspace requires additional funding. The growth of the evaluation portion of the NIAP has relegated other functions to a back burner. NSA is predominantly doing the oversight of evaluations by themselves, while NIST is predominantly working the lab certifications through NVLAP. This leaves the other original functions of the NIAP unattended. Each option carries its set of requirements, and detailed cost estimates should be obtained through the NIAP for the option that will be exercised. Even if funding increases, the personnel shortages discussed above limit the solution in the near term.

8.8.2.3 Research

The topic of research in general is very broad. The NIAP should pursue research that is limited to evaluation-related areas such as metrics, test development, composability, assurance methods, vulnerability characterization, and tool development process. However, under Options 3 through 5 this would include a general awareness of other research in cybersecurity. The independent assessment group of Option 6 may take this up, if that option is implemented.

8.8.2.3 Education, Training, and Awareness

Education, training, and awareness should be for the benefit of all stakeholders and the general consumer of IA products and not limited to evaluation personnel.

8.8.2.3 Metrics and Tracking Systems

A high priority should be placed on developing the metrics that will provide return on investment for evaluated products. Once identified and defined, tracking systems must be put into place and the data should be reported at least annually in assessment reports.

8.8.2.3 Protection Profile Development

It is not intended that the NIAP develop all protection profiles. Rather, facilitation of their production through industry consortia and academic partners should be pursued. The current facilitation between the NIAP and NSA for DoD is a good model of cooperation but a poor model of where responsibility lies. It is often difficult for the consumer to separate NSA effort in this area from the NIAP itself.

8.8.3 Security Support Group (SSG)

Options 2 through 5 all recommend establishing an SSG. The SSG is intended to be a part of the NIAP structure. The tasking of this SSG varies throughout the options and is generally additive up to Option 6, where the group providing independent assessments may subsume the responsibilities. The ISO CC standard creates a global market for secure products because of mutual recognition. Some of the above recommendations require changes to the ISO version of the CC. As a participant in the international standards development process, the U.S. cannot dictate changes to ISO standards. The NIAP (or the independent assessment group of Option 6) should decide when it is advisable to push for changes to the ISO standard.

8.8.4 Testing

Stakeholder expectations revealed several NIAP weaknesses. For example, the CC testing of software security functionality and vulnerabilities does not become nearly detailed enough until levels above EAL4. Most stakeholders prefer or anticipate detailed testing for these at all levels.

8.8.5 Flaw Remediation and Assurance Maintenance

While stakeholders (during interviews) did not discuss flaw remediation, assurance maintenance certainly was discussed. The literature search (as detailed in Chapter 5) provided for flaw remediation as an expectation. The software development cycle currently consists of releases and fixes and possible service packs, which are rollups of fixes. The current CC has provisions for both flaw remediation and maintenance assurance, but they are not part of any assurance packages, and should be included in all evaluations. The absence of flaw remediation and assurance maintenance makes the evaluation certificate quickly obsolete. Moreover, it makes the integration of evaluations with C&A efforts in Option 5 more difficult because the assurance of subsequent product releases is not addressed. Adding these requirements to PPs or acquisition language, as is

the practice in DoD, is good, and should be continued until all evaluations include these items.

8.8.6 Formalization

The informal nature of the NIAP places it at a decided disadvantage when struggling for prioritized funds and negotiating with other Government and non-government entities. Formalization would indicate a stronger support for the program at the funding level and provide it a stronger basis for funding priorities. It would supply a sponsor, requirements, and oversight. It would also provide the NIAP a stronger position in the international community. This lack of a formal charter is in direct contrast to the Defense-wide Information Assurance Program (DIAP), which is formally chartered by the DoD.[30]

8.8.7 C&A Interface

A number of suggestions are made to bolster the integration between product evaluation and the process of C&A. This reduces duplicative effort and strengthens the overall system evaluation.

8.8.8 Improvement of the NIAP Processes

A few NIAP process improvements are in the roadmap because of their overall importance. The text preceding this analysis contains a more complete list of the NIAP process improvements. Specifically, Chapter 5 suggests numerous improvements to the NIAP process.

8.8.9 Consolidation

Making product evaluation more universally required should reduce costs and foster an environment of greater security. However, specific steps must be taken before requiring this consolidation (see cost reduction below).

8.8.10 Cost Reduction

Cost reduction refers to the cost of evaluation. The NIAP stakeholders expressed severe dissatisfaction with the paperwork burden in evaluating products. Likewise, a more cost-effective method of providing low to moderate security is necessary before making product evaluation more universal (Federal Government-wide and critical infrastructure).

---

[30] See Annex D; section D.1.17 for discussion of DIAP.

8.8.11 Standards

The principle interface for evaluations is the CC standard. However, a number of related standards need to be developed. The specific standards need to be determined in Option 6; however, standardized PPs, standardized assurance packages (beyond those in the CC), and security Application Protocol Interfaces (API) are probably needed.

8.9 Other Considerations

8.9.1 Tradeoffs

There is a tradeoff between the optimism for alternative paradigms as listed in Option 6 and the degree to which funding may be diverted from current cybersecurity evaluations into research. Philosophically, a rapid conversion to an alternative paradigm would indicate the choice of Option 2 and the diversion of saved funds into research to bring about this new paradigm as quickly as possible. Practically, however, no new paradigm has been identified nor are any approaching maturation at this time. Breakthroughs in research are unpredictable. Option 6 allows for the gathering of data, analysis, and a heads-up on maturing approaches. This will provide the least lead-time to effect change.

8.9.2 Centralized Responsibility

The need for an overarching responsibility of the security of the nation's cyberspace is a real one. Currently (as delineated in the text), responsibility for pieces of this problem runs from the Department of Commerce (DoC) through DoD, DHS, and others, with exceptions for some application areas. This not only leads to the potential for conflicts but also adds unnecessarily to complexity and duplication of effort. Conflict resolution may be handled by adjudication to higher authority. Complexity and duplication of effort will be handled by analysis and the production of mandates and guidelines. The Independent Assessment group delineated in Option 6 is intended to undertake this responsibility.

8.9.3 Terminology

Terminology is currently aimed at standards developers, evaluators, and oversight personnel. The term *assurance* was not well understood and often improperly related to strength of security. For example, an EAL2 product might be harder to penetrate than an EAL5 product, yet consumers often incorrectly believe the opposite. In truth, the assurance level does not give any indication of the difficulty of penetrating the product. The assurance level primarily describes how much effort and evidence examination was expended in support of the claims, not the extent to which the product provides IA functionality and strength. The paradigm has shifted from a product's security being a specialty to its being a commodity, and the terminology should follow a more intuitive

and common usage path. For example, products should be rated by home, small business, financial industry, commercial business, Federal Government, defense, defense critical, intelligence, etc. Where either the NIAP or the Independent Assessment group would be the keeper of the definition (and definitions are developed by user consortiums), then education and training of consumers would be simplified and the consumer would have an intuitive feel for the product's strengths. These definitions might embody both assurance and strength of security. While the recommendation includes a shift in language, it is not suggested to remove content from the message, and the complexities of the tradeoffs between risk and security should be adequately described in order to not dumb down the language for popular consumption.

8.9.4 Standardized APIs

The advice and consent described under Option 5 is a key element in the integration of product evaluations with C&A. The proper setup of environments, configuration control, and the development of "glue logic" are all key to reduced vulnerabilities in software. The advice and consent will provide an analysis whereby the security of evaluated products is not compromised by its integration into a system's environment. "Glue Logic" comprises the small scripts and programs that reformat and supplement/modify/combine a program's output to be compatible with another program's use. In complex systems (that use many interacting products), these are almost always needed. A concerted program of standardization of APIs for security-enabled software can reduce their use (see section 3.2.2 on standards).

8.9.5 Requirements beyond MRA

Several of the options include elements that extend beyond the current MRA; for example, inclusion of maintenance assurance and flaw remediation, and requiring the use of source code analysis tools. Maintenance assurance and flaw remediation are already part of the CC, but evaluations are not required to address them. Standards for analysis tools would have to be established before their use could be mandated under an MRA.

If additional requirements like these cannot be incorporated under the MRA, they can still be added as U.S. evaluation requirements. NSA has protection profiles that require vulnerability testing (AVA_VLA3), which goes beyond EAL4 evaluations. NSA accepts evaluations of EAL4 products under the MRA, but then requires additional testing by NSA or a U.S. lab to satisfy these PPs.

8.10 DoD and DHS Recommended Actions to Prepare for the Roadmaps

A number of actions by DoD and DHS are recommended to achieve the most useful approach to cybersecurity, which is embodied in a combination of Options 5 and 6.

1. It is recommended that DoD continue to:

a. Develop Protection Profiles (PPs) for DoD and National Security applications;

b. Require conformance to PPs, where available;

c. Require enhanced vulnerability testing in lower-level EAL packages; and

d. Include aspects of flaw remediation and assurance maintenance in PPs.

2. Additionally, it is recommended that DoD:

   a. Require product evaluations to include maintenance assurance and flaw remediation packages of the Common Criteria;

   b. Support the full integration of product evaluation and C&A processes;

   c. Support the development and use of software tools for vulnerability analyses;

   d. Participate in an annual assessment and review of the nation's cybersecurity posture; and

   e. Support the development of a lower cost, alternative form of assurance for lower assurance products (vulnerability analysis tools needed).

3. It is recommended that DHS:

   a. Support vulnerability testing of all products undergoing evaluation;

   b. Support product evaluations to include maintenance assurance and flaw remediation.

   c. Support the full integration of product evaluation and C&A processes;

   d. Support the development and use of software tools for vulnerability analyses;

   e. Support the development of a lower cost, alternative form of assurance for lower assurance products;

   f. Support the development of a set of core functionality protection profiles for use by federal departments and agencies, by critical infrastructure components, and by the commercial sector;

   g. Support the use of core protection profiles, where applicable, to give product buyers confidence in the product's security functionality and suitability for use; and

   h. Support the full integration product evaluation and C&A processes for federal departments and agencies and critical infrastructure components (vulnerability analysis tools **and** a lower cost alternative form of assurance needed).

Annex A. References and Bibliography

[ABRAMS2004] Security in Large System Acquisition, by Marshall Abrams, Joe Veoni, and R. Kris Britton, presented at the 3rd International Conference on COTS-Based Software Systems, February 2004.

[ABRAMS2004] Security in Large System Acquisition: Briefing Slidesams, Joe Veoni, and R. Kris Britton, MITRE Corporation, 2004.

[AFCIO2002] AF-CIO Policy Memorandum 02-14; Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, Attachment 1, Rules, May 27, 2002.

[ATIS2000] ATIS Telecommunications Glossary 2000, T1.523-2001, Prepared by Alliance for Telecommunications Industry Solutions (ATIS) Committee T1A1: Performance and Signal Processing, http://www.atis.org/tg2k/.

[BERINATO2000] Berinato, Scott, The Truth About Cyberterrorism, CIO Magazine, 15 March 2002. http://www.cio.com/archive/031502/truth.html

[BITS2004] BITS Financial Services Roundtable, Highlights from Final CISWG "Phase II" Meeting, 17 November 2004.

[BROADWEL2002] Broadwell, Pete and Emil Ong. A Comparison of Static Analysis and Fault Injection Techniques for Developing Robust System Services, Technical Report, Computer Science Division, University of California, Berkeley, May 2002. http://www.cs.berkeley.edu/~pbwell/papers/saswifi.pdf

[BRAY2002] Bray, Brandon. February 2002. "Compiler Security Checks In Depth." Microsoft Corporation. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dv_vstechart/html/vctchCompilerSecurityChecksInDepth.asp. Retrieved April 29, 2005.

[CC1997] Common Criteria, Common Evaluation Methodology for Information Technology Security, CEM – 97/017, Part 1: Introduction and General Model, Version 0.6, January 11, 1997.

[CC1999] Common Criteria, Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CC2000] Common Criteria, Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, May 2000.

[CC2002] Common Criteria, Common Methodology for Information Technology Security Evaluation, Supplement: ASE – Security Target Evaluation, CCIMB-2002-04-011, May 2002.

[CC2004] Common Methodology for Information Technology Security Evaluation Methodology, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-004.

[CC2004a] Common Criteria, Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2.2, CCIMB-2004-01-001, January 2004. http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part1.pdf

[CC2004b] Common Criteria, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.2, CCIMB-2004-01-002, January 2004. http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part2.pdf

[CC2004c] Common Criteria, Common Methodology for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 2.2, CCIMB-2004-01-003, January 2004. http://niap.nist.gov/cc-scheme/cc_docs/cc_v22_part3.pdf

[CC2004d] Common Criteria Project. Common Methodology for Information Technology Security Evaluation, Version 2.2, CCIMB-2004-01-004, January 2004. http://niap.nist.gov/cc-scheme/cc_docs/cem_v12.pdf

[CC2004e] Common Criteria Project. Assurance Continuity: CCRA Requirements. Version 1.0, CCIMB-2004-02-009, February 2004. http://niap.nist.gov/cc-scheme/cc_docs/assur_con_v1.pdf

[CCA1996] Clinger-Cohen Act of 1996, (formerly the Information Technology Management Reform Act of 1996), Public Law 104-106, August 8, 1996. http://www.defenselink.mil/nii/org/cio/doc/CCA-Book-Final.pdf

[CCEVS11999] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS22000] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS32002] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 1.0, February 2002.

[CCEVS42001] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001.

[CCEVS 52000] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, 31 August 2000.

[CDIDX2004] Chemical Industry Data Exchange (CIDX) Cybersecurity Practices and Standards Guidance Development Guideline, Revision 6, April 19, 2004. http://www.cidx.org/CyberSecurity/publications/Guidance_Development_Guideline.doc.

[CIA1999] Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems, DCID 6/3, June 5, 1999.

[COWAN1998] Cowan, C.; Pu, C.; Maier, D.; Hinton, H. "StackGuard: automatic adaptive detection and prevention of buffer-overflow attacks." In: Proceedings of the Seventh USENIX Security Symposium. Berkeley, CA, USA: USENIX Assoc, 1998. p. 63–77. Conference Paper. http://www.cse.ogi.edu/DISC/projects/immunix/stackguard_usenix98.ps.gz

[COWAN1999] Cowan, Crispin, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade." Proceedings of DARPA Information Survivability Conference and Expo (DISCEX). vol.2. Las Alamitos, CA, USA: IEEE Computing. Soc, 1999. p. 119–29 vol2. ISBN 0-7695-0490-6. http://crispincowan.com/~crispin/discex00.pdf

[COWAN2001a] Crispin Cowan, Steve Beattie, Chris Wright, and Greg Kroah-Hartman. "RaceGuard: Kernel Protection From Temporary File Race Vulnerabilities." Presented at the 10th USENIX Security Symposium, Washington D.C., August 2001. http://crispincowan.com/~crispin/raceguard.pdf

[COWAN2001b] Crispin Cowan, Matt Barringer, Steve Beattie, Greg Kroah-Hartman, Mike Frantzen, and Jamie Lokier. "FormatGuard: Automatic Protection From print Format String Vulnerabilities." Presented at the 10th USENIX Security Symposium, Washington D.C., August 2001. http://crispincowan.com/~crispin/formatguard.pdf

[COWAN2003] Cowan, Crispin. Software Security for Open-Source Systems. IEEE Security and Privacy, 2003. http://www.wirex.com/~crispin/opensource_security_survey.pdf

[CRS2002] Congressional Research Service, "Critical Infrastructures: What Makes an Infrastructure Critical," CRS RL31556, August 30, 2002. http://www.fas.org/irp/crs/RL31556.pdf

[CRS2004] Congressional Research Service, "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives," by John Moteff, CRS RL32357, April 16, 2004. http://www.fas.org/irp/crs/RL32357.pdf

[CRS2004a] The National Institute of Standards and Technology: An Overview, Wendy H. Schacht, Congressional Research Service, Updated 1 December 2004.

[CSEC1988] Computer Security Act of 1987, Public Law 100-235, H.R. 145, January 8, 1988, (has been superseded by Federal Information Security Management Act of 2002 (Title III of E-Gov)).

[CSIA2004] NIAP Certification: Proposals by CSIA for Strengthening Security Certification, Cyber Security Industry Alliance (CSIA), 23 July 2004. https://www.csialliance.org/resources/pdfs/CSIA_NIAP_Recommendations.pdf

[DAA2001] Defense Authorization Act, Title X, Government Information Security Reform Act, Public Law 106-398, February 9, 2001.

[DACOSTA2003] DaCosta, Dan, Christopher Dahn, Spiros Mancoridis, and Vassilis Prevelakis. Characterizing the 'Security Vulnerability Likelihood' of Software Functions IEEE Proceedings of the 2003 International Conference on Software Maintenance (ICSM'03), Amsterdam, The Netherlands, September, 2003. http://www.prevelakis.net/Papers/ICSM03.pdf

[Denning1999] Denning, D.E., Information Warfare and Security, Addison-Wesley, 1999.

[DHS2005] Department of Homeland Security Authorization Act for Fiscal Year 2005, 19 July 2004. http://www.theorator.com/bills108/hr4852.html

[DIP2000] Defense Information Program, 10 USCS Section 2224, (Public Law 106-344), October 20, 2000.

[DoD1982] Department of Defense, Computer Security Evaluation Center, DoD Directive 5215.1, October 25, 1982. http://www.dtic.mil/whs/directives/corres/html/52151.htm

[DoD1985] Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, December 1985. http://jcs.mil/htdocs/teinfo/directives/soft/ds5200.281.html

[DoD1997] Department of Defense, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), DoD Instruction 5200.40, December 30, 1997. http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

[DoD2000] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Department of Defense Global Information Grid Information Assurance, June 16, 2000, superseded by DoD Directive 8500.1, Information Assurance, 24 October 2002. http://www.dtic.mil/whs/directives/corres/pdf2/d85001p.pdf

[DoD2000a] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 4-8460, Department of Defense Global Information Grid Information Networks, August 24, 2000, superseded by DoD Directive 8100.1, Global Information Grid (GIG) Overarching Policy, 19 September 2002. http://www.dtic.mil/whs/directives/corres/html/81001.htm

[DoD2000b] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 8-8001, Global Information Grid, March 31, 2000, superseded by DoD Directive 8100.1, Global Information Grid (GIG) Overarching Policy, 19 September 2002. http://www.dtic.mil/whs/directives/corres/html/81001.htm

[DoD2002] Department of Defense, Global Information Grid (GIG) Overarching Policy, DoDD 8100.1, September 19, 2002. http://www.dtic.mil/whs/directives/corres/html/81001.htm

[DoD2002a] Department of Defense, Information Assurance (IA), DoD Directive 8500.1, October 24, 2002. http://www.dtic.mil/whs/directives/corres/pdf2/d85001p.pdf

[DoD2003a] Department of Defense, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process, Program Manual, DoD O-8530.1-M, December 17, 2003.

[DoD2003b] Department of Defense, Information Assurance (IA) Implementation, DoD Instruction 8500.2, February 6, 2003. http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf

[DoD2004] CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND), Enclosure A: General Information, 15 June 2004. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf

[DSB1999] Report of the Defense Science Board Task Force on Globalization and Security, December 1999. http://www.acq.osd.mil/dsb/globalization.pdf

[DSB2001] Protection the Homeland, Report of the Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, Volume 2, March 2001. http://www.acq.osd.mil/dsb/dio.pdf

[EM2001] M-01-08, Memorandum for the Heads of Executive Departments and Agencies, Guidance on Implementing the Government Information Security Reform Act, General Overview, January 16, 2001. http://www.whitehouse.gov/omb/memoranda/m01-08.pdf

[EM2001a] M-01-24, Memorandum for the Heads of Executive Departments and Agencies, Reporting Instructions for the Government Information Security Reform Act, June 22, 2001. http://www.whitehouse.gov/omb/memoranda/m01-24.pdf

[EO1981] Executive Order, EO 12333, United States Intelligence Activities, 4 December 1981. http://www.cia.gov/cia/information/eo12333.html

[EO1995] Executive Order, EO 12958, Classified National Security Information, 17 April 1995. http://www.dss.mil/seclib/eo12958.htm

[EO1996] Executive Order, EO 13010, Critical Infrastructure Protection, (Federal Register Vol. 61, No. 138), July 15, 1996. http://www.ntia.doc.gov/osmhome/cip/eo13010.pdf

[EO2001] Executive Order, EO 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr18oc01-139.pdf

[EO2003] Executive Order, EO 13286, Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, 28 February 2003. http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-5343.pdf

[ERICKSON2003] Erickson, J., "Hacking: The Art of Exploitation." No Starch Press, 2003.

[FESTA2001] Festa, Paul. November 28, 2001. "The root of the problem: Bad software." http://news.com.com/2008-1082-276316.html?legacy=cnet

[FISCHER2002] Fischer, Eric A, "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options," RL3277, 22 February 2002.

[FISMA2002] The Federal Information Security Management Act of 2002, H.R. 2458, 2002. http://csrc.nist.gov/policies/FISMA-final.pdf

[FORRESTER2000] Forrester, Justin E. and Barton P. Miller. 2000. "An Empirical Study of the Robustness of Windows NT Applications Using Random Testing." ftp://ftp.cs.wisc.edu/paradyn/technical_papers/fuzz-nt.pdf

[GAO1997] GAO's Business Process Reengineering Assessment Guide, Version 3, GAO/AIMD.10.1.15, April 1997. www.gao.gov/special.pubs/bprag/bprgloss.htm

[GAO1999] General Accounting Office, "Certification Requirements: New Guidance Should Encourage Transparency in Agency Decision-making," GAO/GGD-99-170, September 1999. http://www.cpc-online.net/Accomplishments/GAO-GGD-99-170.pdf

[GAO2003] General Accounting Office, "High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures," GAO-03-121, January 2003. http://www.gao.gov/pas/2003/d03121.pdf

[GAO2003a] General Accounting Office, "Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements," GAO-03-852T, June 24, 2003. http://www.gao.gov/new.items/d03852t.pdf

[GAO2004] General Accounting Office, "Information Security: Technologies to Secure Federal Systems, GAO-04-467," March 2004. http://www.gao.gov/new.items/d04467.pdf

[GAO2004a] General Accounting Office, "Information Security: Continued Efforts needed to Sustain Progress in Implementing Statutory Requirements," GAO-04-483t, March 16, 2004. http://www.gao.gov/new.items/d04483t.pdf

[GAO2004b] General Accounting Office, "Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risk," GAO-04-678, May 2004. http://www.gao.gov/new.items/d04678.pdf

[GAO2004c] General Accounting Office, Technology Assessment: Cybersecurity for Critical Infrastructure Protection, GAO-04-321, May 2004. http://www.gao.gov/new.items/d04321.pdf

[GAO2004d] Government Accountability Office, "Information Security: DoD's Acquisition Policies and Guidance Need to Incorporate Additional Best Practices and Controls," GAO-04-722, July 2004. http://www.gao.gov/new.items/d04722.pdf

[GAO2004e] General Accounting Office, "Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation," GAO-04-376, June 2004. http://www.gao.gov/new.items/d04376.pdf

[GAO2004f] General Accounting Office, "Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems," GAO-04-354, March 2004. http://www.gao.gov/new.items/d04354.pdf

[GLB1999] Gramm-Leach-Bliley Act of 1999, Financial Privacy, Public Law 106-102, 12 November 1999. http://banking.senate.gov/conf/

[HIPPA1996] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 21 August 1996. http://aspe.hhs.gov/admnsimp/pl104191.htm

[Howard2002] Howard, M. and LeBlanc, D. (2002), "Writing Secure Code." Microsoft Press, 2002.

[HOWARD2002a] Howard, M. and LeBlanc, D. (2002), "Writing Secure Code." Microsoft Press, December 2002. Second edition. ISBN 0735617228.

[HSA2002] Homeland Security Act of 2002, Title II-Information Analysis and Infrastructure Protection, (Public Law 107-296), H.R. 5005, November 19, 2002. http://www.dhs.gov/interweb/assetlibrary/hr_5005_enr.pdf

[HSPD2003] Homeland Security Presidential Directive, HSPD-7, Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[Huang2003] Huang, A., "Hacking the XBox," No Starch Press, 2003.

[HUMPHREY2003] Humphrey, W. and Davis, N., "Requirements for a Secure Software Development Process," Software Engineering Institute, 24 December 2003.

[IATF2002] Information Assurance Technical Framework, IATF, Release 3.1, September 2002. http://www.iatf.net/framework_docs/version-3_1/index.cfm

[IEEE 1995] Institute of Electrical and Electronics Engineers (IEEE) Computer Society, Portable Applications Standards Committee, "Draft Guide to the POSIX Open System Environment," P1003.0/D18, Feb. 1995, pp. 13–18.

[IEEE2002] IEEE 610.12, IEEE Standard Glossary of Software Engineering Terminology, 1990, revised 2002.

[ISO1996] ISO/IEC Guide 65, General Requirements for Bodies Operating Product Certification Systems, 1996. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26796&ICS1=3&ICS2=120&ICS3=20

[ISO1996a] ISO/IEC Guide 2: Standardization and related activities- general vocabulary, 1996. http://www.tc67.addr.com/teched/typeformcontent.htm#isoguide2

[ISO1999] ISO/IEC 17025, General Requirements for the Competence of Testing and Calibration Laboratories, 1999. http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30239&ICS1=3

[ISO1999a] ISO/IEC 15408-1, Information Technology – Security Techniques – Evaluation Criteria for IA Security – Part 1: Introduction and General Model, First Edition, 1 December 1999. http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=27632&ICS1=35

[ISO2003] ISO/IEC DTR15446, Information Technology – Security Techniques – Guide for the Production of Protection Profiles and Security Targets, 2003.

[ISO2005] ISO/IEC 17025, General Requirements for the Competence of Testing and Calibration Laboratories, 2005. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39883&ICS1=3&ICS2=120&ICS3=20

[ISPAB2004] The National Institute for Standards and Technology Computer Security Division: The Case for Adequate Funding, A Report by the Information Security and Privacy Advisory Board, June 2004.

[ITMRA1996] Information Technology Management Act of 1996, superseded by Clinger-Cohen Act. http://govinfo.library.unt.edu/npr/library/misc/s1124.html.

[JACKSON2004] Jackson, Joab. July 19, 2004. "Linux now a corporate beast." Government Computer News. http://www.gcn.com/vol1_no1/daily-updates/26641-1.html

[Karger 2004] Karger, Paul A., and Helmut Kurth. Increased Information Flow Needs for High-Assurance Composite Evaluations. 2nd IEEE International Information Assurance Workshop, Charlotte, NC, April 8-9, 2004. Also presented at 4th Annual High Confidence Software and Systems Conference, Baltimore, MD, April 13–15, 2004. IBM Research Report RC 22950 (W0310-168), Revision 2, 30 October 2003. http://domino.watson.ibm.com/library/cyberdig.nsf/1e4115aea78b6e7c85256b360066f0d4/ba891c1b75396d4485256e280055a1f1?OpenDocument&Highlight=0,karger

[Kleen2004] Kleen, Andy. http://www.thisishull.net/archive/index.php/t-3810.html. Retrieved April 29, 2005

[LIPNER2005] Lipner, Steve and Michael Howard. March 2005. "The Trustworthy Computing Security Development Lifecycle." http://msdn.microsoft.com/security/default.aspx?pull=/library/en-us/dnsecure/html/sdl.asp#sdl2_topic5_2. Retrieved April 29, 2005

[McClure2003] McClure, S., Scambray, J., and Kurtz, G., "Hacking Exposed: Network Security Secrets and Solutions," 4th Ed. Osborne, 2003.

[MCGRAW2000] McGraw, Gary and John Viega. March 1, 2000. "Make Your Software Behave: Learning the Basics of Buffer Overflows." IBM developer Works. http://www-

128.ibm.com/developerworks/security/library/s-overflows/index.html

[MILLER1990] Miller, Barton P., Lars Fredriksen and Bryan So. "An Empirical Study of the Reliability of UNIX Utilities." ftp://ftp.cs.wisc.edu/paradyn/technical_papers/fuzz.pdf

[MILLER1995] Miller, Barton P., David Koski, Cjin Pheow Lee, Vivekananda Maganty, Ravi Murthy, Ajitkumar Natarajan, and Jeff Steidl. 1995. "Fuzz Revisited: A Re-examination of the Reliability of UNIX Utilities and Services." ftp://ftp.cs.wisc.edu/paradyn/technical_papers/fuzz.pdf

[MITRE 2003] MITRE. January 2, 2003. Use of Free and Open-Source Software (FOSS) in the US Department of Defense. http://www.egovos.org/rawmedia_repository/588347ad_c97c_48b9_a63d_821cb0e8422d?/document.pdf

[NBSA1901] National Bureau of Standards Act, 15 U.S.C. 278g-3, March 3, 1901, as modified by The Computer Security Act of 1987, Public Law 100-235, (H.R. 145), January 8, 1988. http://www.ssa.gov/OP_Home/comp2/F100-235.html

[NCC1996] National Computer Center, Certification and Accreditation Process Handbook for Certifiers, Version 1, NCSC-TG-031, ISWG-9608-28, July 1996. http://iase.disa.mil/ditscap/CA_Handbook.doc

[NCSG1990] NCSC-TG-002, Trusted Product Evaluations – A Guide for Vendors, (Bright Blue Book), Version 1, Library No. S-228, 538, June 22, 1990. http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-002.html

[NDA2002] National Defense Authorization Act for Fiscal Year 2003, Subtitle F – Information Technology, Section 352, Public Law 107-314, H.R. 4546, December 2, 2002. http://carper.senate.gov/acrobat%20files/FS061902.pdf

[NIAC2004] National Infrastructure Advisory Council, Vulnerability Disclosure Framework, Final Report and Recommendations by the Council, 13 January 2004.

[NIAP1999] NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Organization, Management and Concept of Operations) Scheme Publication #1, Version 2.0, May 1999. http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-1.pdf

[NIAP2000a] NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Validation Body Standard Operating Procedures), Scheme Publication #2, Version 1.5, May

2000. http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-2.pdf

[NIAP2000b] NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to Sponsors of IT Security Evaluations) Scheme Publication #5, Version 1.0, August 31, 2000. http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-5.pdf

[NIAP2001] NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to CCEVS Approved Common Criteria Testing Laboratories) Scheme Publication #4, Version 1.0, March 20, 2001. http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-4.pdf

[NIAP2002] NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to Validators of IT Security Evaluations) Scheme Publication #3, Version 1.0, February 2002. http://niap.nist.gov/cc-scheme/policy/ccevs/scheme-pub-3.pdf

[NIAP2003] NIAP Common Criteria Evaluation and Validation Scheme. Jean H. Schaffer. NIAP. http://www.secure-biz.net/Conference2003/presentations/NIAP%20Brief%20for%20E-summit(schaffer).ppt

[NISTn.d.] Interagency Agreement between the National Institute of Standards and Technology's Computer Security Division and the Department of Homeland Security's National Cyber Security Division, n.d.

[NIST1983] NIST, FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, September 27, 1983. http://csrc.nist.gov/publications/fips/

[NIST2000] NIST, SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, Recommendations of the National Institute of Standards and Technology, (Edward A. Roback) August 2000. http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf

[NIST2001] NIST, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Category: Computer Security, Subcategory: Cryptography, May 25, 2001. http://csrc.nist.gov/publications/fips/

[NIST2001a] NIST, Handbook 150, National Voluntary Laboratory Accreditation Program Procedures and General Requirements, 2001 Edition, July 2001.

[NIST2002a] NIST, Handbook 150-20, National Voluntary Laboratory Accreditation Program, Information Technology Security Testing-Common Criteria, Draft Version 5, (Jeffrey Horlick, Roberta

Medlock, Patricia Toth), May 2002. http://niap.nist.gov/cc-scheme/policy/ccevs/HB150-20.pdf

[NIST2002b] NIST, SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, Initial Public Draft, Version 1.0, (Ron Ross, Marianne Swanson), October 2002, SP 800-37.

[NIST2003] NIST, SP 800-36, Guide to Selecting Information Technology Security Products, Recommendations of the National Institute of Standards and Technology, (Timothy Grance, Marc Stevens, Marissa Myers) October 2003. http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[NIST2003a] NIST, SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003. http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

[NIST2003b] NIST, SP 800-35, Guide to Information Technology Security Services, October 2003.

[NIST2004] NIST, SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, Version 1.0, (Ron Ross, Marianne Swanson), May 2004, SP 800-37. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

[NIST/NSA1997] NIST/NSA Letter of Partnership, 22 August 1997.

[NIST/NSA1998] NIST/NSA Terms of Reference for the National Information Assurance Partnership between NIST and NSA ISSO, 6 July 1998.

[NSIA2004] National Cyber Security Partnership, Technical Standards and Common Criteria Task Force: Recommendations Report, April 2004. http://www.cyberpartnership.org/TF4TechReport.pdf

[NSD1990] NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, July 5, 1990. http://www.fas.org/irp/offdocs/nsd/nsd_42.htm

[NST1994] NSTISSP No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems, April 8, 1994. http://www.nstissc.gov/Assets/pdf/NSTISSP%20_.6.pdf

[NST1999] NSTISSAM COMPUSEC/1-99, Advisory on the Transition From the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation, March 11, 1999. http://www.nstissc.gov/Assets/pdf/NSTISSAM_INFOSEC1-99.pdf

[NST2000] NSTISSAM INFOSEC/2-00, Advisory Memorandum For the Strategy For Using the National Information Assurance Partnership (NIAP) For the Evaluation of Commercial Off-The-Shelf (COTS) Security Enabled Information Technology Products, February 8, 2000. http://www.nstissc.gov/Assets/pdf/nstissam_infosec_2-00.pdf

[NST2000a] NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000. http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf

[NST2000b] NSTISSP No. 11, FACT Sheet, National Information Assurance Acquisition Policy, January 2000. http://niap.nist.gov/cc-scheme/nstissp11_factsheet.pdf

[NST2000c] NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, September 2000, NSTISSI No. 4009.

[NST2002] NSTISSP No. 11, Annex A, NSTISSP No. 11 Deferred Compliance Authorizations (DCAs), Version 1.10, 18 October 2002.

[NST2003] NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, Revised, June 2003.

[NSTAC2004] The President's National Security Telecommunications Advisory Committee (NSTAC) Fact Sheet, revised 1/28/04.

[OMB1996] Office of Management and Budget, Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, Revised, February 8, 1996. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

[OMB2001] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, Guidance on Implementing the Government Information Security Reform Act, OMB Memorandum M-01-08, January 16, 2001. http://www.whitehouse.gov/omb/memoranda/m01-08.pdf

[OMB2003] Office of Management and Budget, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, OMB Memorandum M-03-19, August 6, 2003. http://www.whitehouse.gov/omb/memoranda/m03-19.pdf

[OMB2004] Office of Management and Budget, FY2003 Report to Congress on Federal Government Information Security Management, March 1, 2004. http://www.whitehouse.gov/omb/inforeg/fy03_fisma_report.pdf

[OMB2004a] Office of Management and Budget, FY2003 Report to Congress on Implementation of the E-Government Act, March 8, 2004. http://www.whitehouse.gov/omb/egov/fy03_egov_rpt_to_congress.pdf

[OWASP 2004] Open Web Application Security Project (OWASP) Top Ten Project. January 27, 2004. The Ten Most Critical Web Application Security Vulnerabilities: 2004 update. http://www.owasp.org/documentation/topten.html. Retrieved May 3, 2005.

[PDD1998] Presidential Decision Directive 63, Critical Infrastructure Protection, May 22, 1998. http://www.fas.org/irp/offdocs/pdd-63.htm

[PETERSON2004] What's in a Name? by Rodney Peterson with Ronald Larsen, Corey Schou, and Lee Strickland, Educause Quarterly, Number 3, 2004. http://www.educause.edu/ir/library/pdf/eqm0430.pdf

[PRA1995] Paperwork Reduction Act of 1995, 22 May 1995. http://www.cio.noaa.gov/itmanagement/pralaw.pdf

[PRIETO-DIAZ2002] The Common Criteria Evaluation Process: Process Explanation, Shortcomings, and Research Opportunities, Commonwealth Information Security Center Technical Report CISC-TR-2002-003, James Madison University, December 2002.

[QUALITYn.d.] Sacramento County Office of Quality and Strategic Planning Glossary, n.d. http://hra.co.sacramento.ca.us/quality/Quality/glossary.htm

[RUBIN2001] Rubin, A., The Whitehat Security Arsenal: Tackling the Threats. Addison-Wesley, 2001.

[SECURE2004] Secure Software. Services Overview. Retrieved May 24, 2004. http://www.securesoftware.com/services_overview.htm

[SOA2002] Sarbanes-Oxley Act, Public Company Accounting Reform and Investor Protection Act, Public Law 107-204, 30 July 2002. http://www.pcaobus.org/rules/Sarbanes_Oxley_Act_of_2002.pdf

[Spitzner2003] Spitzner, L., Honeypots: Tracking Hackers. Addison-Wesley, 2003.

[SYMANTEC2005] Symantec. "W32.Bofra.E@mm" Last Updated on: March 15, 2005. Retrieved April 29, 2005. http://securityresponse.symantec.com/avcenter/venc/data/w32.bofra.e@mm.html

[TEVIS2004] Tevis, by Jay-Evan J. Tevis and John A. Hamilton. Methods for the prevention, detection and removal of software security vulnerabilities. Proceedings of the 42nd annual Southeast regional

conference, Huntsville, Alabama, 2004 (Pages: 197–202). ISBN 1-58113-870-9/04/04.

[TORVALDS2004] Torvalds, Linus. Nov 14, 2004. "Re: [PATCH] init in mm/slab.c," Linux kernel mailing list. http://www.ussg.iu.edu/hypermail/linux/kernel/0411.1/1781.html

[USAF2002] U.S. Air Force, Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, AF-CIO Policy Memorandum 02-14, May 27, 2002.

[USCERT] U.S. CERT. "Microsoft Internet Explorer vulnerable to buffer overflow via FRAME and IFRAME elements." Vulnerability Note VU#842160. http://www.kb.cert.org/vuls/id/842160

[VANDEVEN2005] van de Ven, Arjan. August 2004. "New Security Enhancements in Red Hat Enterprise Linux" v.3, update 3. http://www.redhat.com/f/pdf/rhel/WHP0006US_Execshield.pdf. Retrieved April 29, 2005

[Viega2002] Viega, J. and McGraw, G., Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley, 2002.

[Waltz1998] Waltz, E., Information Warfare: Principles and Operations, Artech House, 1998.

[WHEELER2002] Wheeler, David A. July 29, 2002. "More Than a Gigabuck: Estimating GNU/Linux's Size." http://www.dwheeler.com/sloc

[WHEELER2003] Secure Programming for Linux and Unix HOWTO. 3 March 2003. http://www.dwheeler.com/secure-programs/

[WH2002] White House, National Security Strategy of the United States of America, September 2002. http://www.whitehouse.gov/nsc/nss.html

[WH2002a] White House, National Strategy for Homeland Security, Office of Homeland Security, July 2002. http://www.whitehouse.gov/homeland/book/

[WH2003] White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003. http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

[WH2003a] White House, National Strategy to Secure Cyberspace, February 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[Whittaker2004] Whittaker, J.A. and Thompson, H.H., How to Break Software Security. Addison-Wesley, 2004.

[WILANDER2002a] Wilander, John and Mariam Kamkar. A Comparison of Publicly Available Tools for Static Intrusion Prevention, 75th Nordic Workshop on Secure IT Systems, 2002, Karlstad, Sweden.

http://www.ida.liu.se/~johwi/research_publications/paper_nordsec2002_john_wilander.pdf

[WILANDER2002b] Wilander, John. Security Intrusions and Intrusion Prevention, Master's Thesis. April 15, 2002. Linkopings universitet, Sweden.

[WILANDER2003] Wilander, John and Mariam Kamkar. A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention. 75th Nordic Workshop on Secure IT Systems, 2002, Karlstad, Sweden.

[Wu 2004] Information Security in the Federal Government: One Year into the Federal Information Security Management Act, Statement of Ben Wu, Deputy Under Secretary Technology Administration, U.S. Department of Commerce Before the Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, U.S. House of Representatives, March 16, 2004.

[ZALEWSKI2004a] Zalewski, Michal. October 18, 2004. "Web browsers - a mini-farce." Bugtraq mailing list. http://www.securityfocus.com/archive/1/378632

[ZALEWSKI2004b] Zalewski, Michal. October 22, 2004. "Update: Web browsers - a mini-farce (MSIE gives in)" Bugtraq mailing list. http://www.securityfocus.com/archive/1/379207

Annex B. Acronyms

A

AMA: Assurance Maintenance Activity
AMP: Assurance Maintenance Plan
ANSI: American National Standards Institute
APNSA: Assistant to the President for National Security Affairs
ASD/NII: Assistant Secretary of Defense Networking and Information Integration
ASTM: American Society of Testing Materials
ATE: Assurance Measures for Testing
AVA: Assurance Vulnerability Assessment

C

C&A: (1) Certification and accreditation (2) Certification and authorization to operate (FAA)
CAE: Centers of Academic Excellence
CB: Certification/validation body
CC: Common Criteria
CCA: Clinger-Cohen Act
CCEB: CC Editing Board
CCEL: Common Criteria Evaluation Laboratory
CCEP: Commercial COMSEC Evaluation Program
CCEVS: Common Criteria Evaluation and Validation Scheme
CCIMB: CC Implementation Management Board
CCRA: Common Criteria Recognition Arrangement
CCTL: Common Criteria Testing Laboratory
CEM: Common Evaluation Methodology
CEMEB: Common Evaluation Methodology Editing Board
CFR: Code of Federal Regulations
CI: Critical Infrastructure
CIA: Central Intelligence Agency
CIAO: Critical Infrastructure Assurance Office
CIO: Chief Information Officer
CIP: Critical Infrastructure Protection
CLEF: Common Criteria Licensed Evaluation Facility
CM: (1) Common Methodology (2) Configuration Management
CMP: Certificate Maintenance Program
CMR: Certificate Maintenance Report
CMSR: Certificate Maintenance Summary Report
CMT LAP: NVLAP® Cryptographic Module Testing Laboratory Accreditation Program
CMV: Cryptographic Module Validation
CMVP: Cryptographic Module Validation Program
CND: Computer Network Defense

CNDS: Computer Network Defense Services
CNSS: Committee on National Security Systems
COMPUSEC: COMPUter SECurity
COMSEC: COMmunications SECurity
COTS: Commercial off-the-shelf
CRS: Congressional Research Service
CSA: Computer Security Act
CSEC: Computer Security Evaluation Center
CSI: Computer Security Institute
CSIA: Cyber Security Industry Alliance
CSD: Computer Security Division
CSTT: Cryptographic Support Test Tool
CTSC: Chenega Technology Services Corporation

D

DAA: (1) Designated Accrediting Authority
(2) Designated Approving Authority
DCA: Deferred Compliance Authorization
DCI: Director of Central Intelligence
DCID: Director of Central Intelligence Directives
DDCI/CM: Deputy Director of Central Intelligence for Community Management
DEA: Drug Enforcement Agency
DHHS: Department of Health and Human Services
DHS: Department of Homeland Security
DIA: Defense Intelligence Agency
DISA: Defense Information Systems Agency
DIACAP: Defense Information Assurance Certification and Accreditation Process
DIRNSA: Director National Security Agency
DITSCAP: DoD Information Technology Security and Certification Process
DLA: Defense Logistics Agency
DOC: Department of Commerce
DoD: Department of Defense. Also used as the tag for stakeholder class of DoD users.
DoDD: DoD Directive
DoDI: DoD Instruction
DSB: Defense Science Board
DTRA: Defense Threat Reduction Agency
DVA: Department of Veteran Affairs

E

E-Gov: E-Government Act
EAL: Evaluation Assurance Level
EAP: Evaluation Acceptance Package
EF: Evaluation facility, an organization that carries out evaluations independently of the developers of the IT products or protection profiles, usually on a commercial basis.

EMSEC: EMissions SECurity
EO: Executive Order
EOP: Executive Office of the President
ESR: Evaluation Summary Report
ET&A: Education, Training, and Awareness
ETR: Evaluation Technical Report

F

FAA: Federal Aviation Administration
FBI: Federal Bureau of Investigation
FCC: Federal Communications Commission
FedNonDoD: Used as the tag for stakeholder class of Federal users that is not DoD.
FEMA: Federal Emergency Management Agency
FFRDC: Federally-Funded Research and Development Center
FIPS: Federal Information Processing Standard
FIRMR: Federal Information Resources Management Regulations
FISMA: Federal Information Security Management Act of 2002
FRS: Federal Reserve System
FTC: Federal Trade Commission

G

GAO: Government Accountability Office (prior to July 7, 2004, the General Accounting Office)
GIG: Global Information Grid
GISR: Government Information Security Reform
GLB: Gramm-Leach-Bliley Act
GOTS: Government off the Shelf
GSA: Government Services Administration

H

HASC: **House Armed Services Committee**
HIPPA: Health Insurance Portability and Accountability Act of 1996
HPSCI: House Permanent Select Committee on Intelligence
HAS: Homeland Security Act
HSPD: Homeland Security Presidential Directive

I

IA: Information Assurance
IATF: Information Assurance Technical Framework
IATFF: Information Assurance Technical Framework Forum
IAW: Indications and Warnings
IC: Intelligence Community
IDA: Institute for Defense Analyses
IEC: International Electro-technical Commission
IEEE: Institute of Electrical and Electronics Engineers
IETF: Internet Engineering Task Force
IG: Inspectors General
INFOSEC: INFOrmation SECurity

INS: Immigration and Naturalization Service
IRA: Intelligence Reform Act
IRTPA: Intelligence Reform and Terrorism Prevent Act 2004
ISPAB: Information Security and Privacy Advisory Board
ISO: International Organization for Standards
ISS: Information Systems Security
IT: Information Technology
ITMRA: Information Technology Management Reform Act of 1996
ITSEC: Information Technology Security Evaluation Criteria
ITSEF: IT Security Evaluation Facility
ITSEM: Information Technology Security Evaluation Manual
ITU: International Telecommunications Union

J

JCS: Joint Chiefs of Staff

K

KPA: Key Process Area

M

MR: (1) Memorandum for Record
(2) Management Representative
MRA: Mutual Recognition Agreement
MSR: Monthly Summary Report

N

NASA: National Aeronautics and Space Administration
NCS: National Communications System
NDAA: National Defense Authorization Act
NDI: Non Developmental Item
NERC: North American Electric Reliability Council
NGA: National Geospatial-Intelligence Agency
NIACAP: National Information Assurance Certification and Accreditation Process
NIAP: National Information Assurance Partnership
NIPC: National Infrastructure Protection Center
NIST: National Institute of Standards and Technology
NRIC: Network Reliability and Interoperability Council of the FCC
NRC: Nuclear Regulatory Commission
NRO: National Reconnaissance Office
NSA: National Security Agency; National Security Act
NSD: National Security Directive
NSF: National Science Foundation
NSI: National Security Information
NSS: National Security Systems
NSTISSAM: National Security Telecommunications and Information Systems Security Advisory/Information Memorandum

NSTISSC: National Security Telecommunications and Information Systems Security Committee (U.S.)
NSTISSI: National Security Telecommunications and Information Systems Security Instruction
NSTISSP: National Security Telecommunications and Information Systems Security Policy
NTTAA: National Technology Transfer and Advancement Act of 1995
NVLAP: National Voluntary Laboratory Accreditation Program

O

OD: Observation Decision
ODRB: Observation Decision Review Board
OMB: Office of Management and Budget
OPM: Office of Personnel Management
OPSEC: OPerations SECurity
OR: Observation Report
OSP: Organizational Security Policy
OSTP: White House Office of Science and Technology Policy

P

PCAOB: Public Company Accounting Oversight Board
PDD: Presidential Decision Directive
POA&M: Plan of Action and Milestones
POC: Point of Contact
POSIX: Portable Operating System Interface
PP: Protection Profile
PRA: Paperwork Reduction Act

R

RA: Registration Authority
RCR: Representation CoRrespondence
RI: Request for Interpretation
ROI: Return on Investment

S

SAR: Security assurance requirement
SASC: Senate Armed Services Committee
SEC: Securities and Exchange Commission
SEI: Software Engineering Institute
SF: Security Function
SFP: Security Function Policy
SFR: Security Functional Requirement
S/L/T: State/Local/Tribal
SOF: Strength of Function
SOX: Sarbanes-Oxley Act
SP: Special Publication
SSA: Sector Specific Agency
SSAA: System Security Authorization Agreement

SSCI: Senate Select Committee on Intelligence
SSE-CMM: System Security Engineering Capability Maturity Model
SSG: Security Support Group
SSP: Scientific Subroutine Package
ST: Security Target
ST&E: Security Test and Evaluation

T

TCSEC: Trusted Computer System Evaluation Criteria
TOE: Target of Evaluation
TPEP: Trusted Product Evaluation Program
TSC: TSF Scope of Control
TSF: TOE Security Functions
TSFI: TSF Interface
TSP: TOE Security Policy
TSS: TOE Summary Specification
TTAP: Trust Technology Assessment Program
TTP: Trusted Third Party

U

UL: Underwriters' Laboratory
USG: U.S. Government

V

VA: Veterans Administration
VID: Validation Identification Number
VPL: Validated Products List
VR: Validation Report

Annex C

Annex D Glossary

C.1 General Terminology

A

Acceptance Phase: Start of an assurance maintenance cycle in which the developer establishes plans and procedures for assurance maintenance that are independently validated by an evaluator.

Accreditation: (1) Formal recognition that a laboratory is competent to carry out specific tests or calibration or types of tests or calibrations. (2) Confirmation by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence. (see section C.2 for context associated with Certification and Accreditation [definition 2])

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Accredited: Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Action: Explicitly described CC evaluator action element or one derived from a specified developer action element.

Activity: Application of a CC assurance class.

A.NOEVIL: Assumption that authorized administrators is non-hostile and follows all administrator guidance; however, they are capable of error.

Applicant: Entity (organization, individual, etc.) requesting the assignment of a register entry and entry label.

Approval Policy: A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme, setting out the procedures for making an application to be approved as a CCTL and placed on the NIAP Approved Laboratories List and for the processing of such applications and of the requirements which an applicant must fulfill in order to qualify.

Approved Lab List: The list of approved CCTLs authorized by the NIAP Validation Body to conduct IT security evaluations within the Common Criteria Evaluation and Validation Scheme.

Approved Test Method List: The list of approved test methods maintained by the NIAP Validation Body, which can be selected by a CCTL in choosing its scope of accreditation, i.e., the types of IT security evaluations that it will be authorized to conduct using NIAP-approved test methods.

Approved: Assessment by a national evaluation body as being technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of the CCEVS.

Assets: (1) Information or resources to be protected by the countermeasures of a TOE; assets may be external to the TOE but within the IT environment. (2) Anything that has value to the organization.

Assignment: Specification of a parameter filled in when an element is used in a Protection Profile (PP) or Security Target (ST).

Assumption: Security aspects of the environment in which the TOE will or is intended to be used.

Assurance: Grounds for confidence that an entity meets its security objectives.

Assurance Maintenance Plan: Part of the formal assurance maintenance documentation submitted to the validation body by the sponsor of an evaluation that identifies the plans and procedures that a developer is to implement in order to ensure that the assurance that was established in the certified/validated TOE is maintained as changes are made to the target of evaluation (TOE) or its environment.

Attack Potential: Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources, and motivation.

Augmented: Addition of one or more assurance components from Part 3 of the CC to an EAL that is not normally part of that EAL.

Authenticity: Property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information.

Authorized User: User who may, in accordance with the TOE security policy (TSP), perform an operation.

Availability: (1) Property of being accessible and usable upon demand by an authorized entity. (2) Prevention of unauthorized withholding of information resources.

B

Baseline Controls: A minimum set of safeguards established for a system or organization.

Best Practices: processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency.

C

Certification: (1) the procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements or standards. (2) a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to

determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certification/validation body: an organization responsible for carrying out certification/validation and for overseeing the day-to-day operation of an evaluation and certification or validation scheme.

Certificate Authorizing Participant: National Evaluation Authority and CCRA signatory that issues CC Certificates and recognizes those issued by other National Evaluation Authorities.

Certificate Consuming Participant: National Evaluation Authority and CCRA signatory that recognizes CC Certificates issued by other National Evaluation Authorities but at present do not issue any certificates itself.

Certificate of Accreditation: Document issued by the National Voluntary Laboratory Accreditation Program (NVLAP®) or other national evaluation authority to a laboratory that has met the criteria and conditions for accreditation. A current Certificate of Accreditation may be used as proof of accredited status and is always accompanied by a Scope of Accreditation.

Certificate Maintenance Program: a program within the CCEVS that allows a sponsor to maintain a CC Certificate by providing a means to ensure that a validated TOE will continue to meet its Security Target as changes are made to the IT product or its environment.

Certificate Maintenance Report: a report prepared by a CCTL for the evaluation authority detailing the results of their evaluation maintenance activities conducted on behalf of a sponsor.

Certificate Maintenance Summary Report: an annual report prepared by a sponsor for the evaluation authority providing a summary of all certificate maintenance activities conducted during the previous year.

Certification/Validation: (1) Process carried out by a CB leading to the issuance of a CC Certificate; (2) comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. (see section C.2 for context information)

Certification/Validation Report: Public document issued by a CB that summarizes the results of an evaluation and confirms the overall results—that is, the evaluation has been properly carried out; the evaluation criteria, evaluation methods, and other procedures have been correctly applied; and the conclusions of the Evaluation Technical Report are consistent with evidence adduced.

CC Certificate: A brief public document issued by the NIAP Validation Body under the authority of NIST and NSA which confirms that an IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has associated with it, a validation report.

Certified TOE: (1) Product or system and its associated guidance that, having been a TOE under evaluation, has completed the evaluation, its ST, certification report, and certificate having been published. (2) Version of TOE that was evaluated, awarded a CC Certificate, and is listed in an evaluation authority's Evaluated Products List.

Certified/Validated Products List: Public document that summarizes and confirms the results of an evaluation and lists current valid CC Certificates in accordance with the CCRA.

Check: Similar to, but less rigorous than, confirm or verify; a quick determination to be made by the evaluator, perhaps requiring only a cursory analysis, or perhaps no analysis at all.

Class: Grouping of security requirements that share a common focus; members of a class are termed families.

Coherent: Entity that is logically ordered and has a discernible meaning; for documentation, this adjective addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.

Common Criteria: Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Certificate: (1) Public document issued by a compliant CB and authorized by a participant that confirms that a specific IT product or Protection Profile has successfully completed evaluation by an IT security evaluation facility (ITSEF); a CC Certificate always has associated with it a certification and validation report. (2) Formal recognition by the NIAP® validation body that the IT security evaluation has been conducted in accordance with the CCEVS requirements using the CC and CM. A product that has received a CC Certificate is placed on NIAP®'s Validated Products List.

Common Criteria Evaluation and Validation Scheme: The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles.

Common Criteria Implementation Management Board: conducted trial evaluations of first draft of CC and developed second draft of CC.

Common Criteria Interpretation Management Board: renders CC interpretations to facilitate consistent evaluation results under the Common Criteria Recognition Agreement (CCRA).

Common Criteria Testing Laboratory: Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.

Common Evaluation Methodology: Common Methodology for Information Technology Security Evaluations – a technical document that describes a set of IT security evaluation methods.

Common Evaluation Methodology Editing Board: CCRA participants involved in development of CEM.

Common Methodology for Information Technology Security Evaluation: a technical document that describes a particular set of IT security evaluation methods, also referred to as CEM.

Communications Security: measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emissions security, and physical security of COMSEC material.

Complete: All necessary parts of an entity have been provided. In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction.

Component TOE: TOE that forms part of a composite TOE; the lowest level TOE in an IT product or system.

Components: Specific set of security requirements that are constructed from elements; the smallest selectable set of elements that may be included in a PP, an ST, or a package.

Composability: Mathematical problem where several evaluated products are used to make up a system. Their security features and metrics and the way they are combined are then used to compute a system security set of metrics. The problem is not yet solved.

Composite TOE: TOE composed of multiple component TOEs; the highest level TOE in an IT product or system.

Computer Security: (1) preventing, detecting, and minimizing the consequences of unauthorized actions by users (authorized and unauthorized) of a computer system. (2) measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Confidentiality: The prevention of unauthorized disclosure of information.

Confirm: To review in detail in order to make an independent determination of sufficiency, with the level of rigor required depending on the nature of the subject matter; applicable to evaluator actions.

Connectivity: Property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Consistent: Relationship between two or more entities, indicating that there are no apparent contradictions between these entities.

Corrective security objective: Security objectives that require the TOE to take action in response to potential security violations or other undesirable events, in order to preserve or return to a secure state and/or limit any damage caused.

Counter: Offset, nullify, defensive response (i.e., a security objective that mitigates a particular threat but does not necessarily indicate that the threat is completely eradicated as a result).

Critical Infrastructure Protection: banking and finance, energy, chemical sites, transportation, telecommunications, Government facilities, dams, national monuments and icons. *cybersecurity* is a key element of infrastructure protection.

Cybersecurity: the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (see section C.2 for context of this and related terms).

Cyberterrorism: a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.

Cryptographic Algorithm Testing: Input/output testing to determine whether the implementation conforms to the specification.

Cryptographic Boundary: Explicitly defined contiguous perimeter that establishes the physical bounds of a cryptographic module

Cryptographic Module: Set of hardware, software, firmware, or a combination thereof that implements cryptographic logic or processes, including cryptographic algorithms and key generation, and is contained within the cryptographic boundary of the module.

Cryptographic Module Validation: the act of determining if a cryptographic module conforms to the requirements of FIPS PUB 140-2.

Cryptographic Module Validation Program: a program run jointly by the Communications Security Establishment (CSE) of the Government of Canada and the National Institutes of Standards and Technology (NIST) that focuses on security conformance testing of a cryptographic module against FIPS PUB 140-2, Security Requirements for Cryptographic Modules, and other related cryptographic standards.

Cryptographic Support Test Tool: used as part of Cryptographic Module Validation Program (CMVP).

Current version of TOE: Version of TOE that differs in some respect from the certified version, such as (1) a new release of the TOE, (2) a certified version with patches to correct subsequently discovered bugs, and (3) the same basic version of the TOE but on a different hardware or software platform.

D

Data Integrity: Property that data has not been altered or destroyed in an unauthorized manner.

Demonstrate: Analysis leading to a conclusion; less rigorous than a proof.

Dependency: Relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Depth: Level of design and implementation that is being evaluated.

Describe: Provide specific details about an entity.

Detective Security Objective: Security objectives that provide the means to detect and monitor the occurrence of events relevant to the secure operation of the TOE.

Determine: Conducting an independent analysis, usually in the absence of any previous analysis having been performed, with the objective of reaching a particular conclusion; differs from confirm or verify, as these terms imply that an analysis has already been performed that must be reviewed.

E

Evaluation Facility: an organization that carries out evaluations independently of the developers of the IT products or protection profiles, usually on a commercial basis.

Element: Indivisible security requirement that can be verified by the evaluation; lowest level security requirement from which components are constructed.

Emissions security: protection resulting from measures taken to deny unauthorized persons information derived from the interception and analysis of compromising emanations from crypto equipment or IT systems.

Entry Label: Naming information that uniquely identifies a registered PP or package.

Evaluation: The assessment of an IT product against the Common Criteria using the Common Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation Acceptance Package: A set of documentation from the CCTL consisting of a complete security target for the Target of Evaluation (TOE) and a complete evaluation work plan detailing the inputs, actions and timelines for the conduct of the evaluation; and the identification of points of contact for both the CCTL and the sponsor of the evaluation.

Evaluation Authority: National body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by CBs within that community.

Evaluation Scheme: *See* Common Criteria Evaluation and Validation Scheme.

Evaluation Summary Report: a report issued by an overseer and submitted to an evaluation authority that documents the oversight verdict and its justification.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to the CCEVS Validation Body as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Evaluator Action Element: Assurance requirement stated in Part 3 of the CC that represents a TOE evaluator's responsibilities in verifying the security claims made in the Security Target of a TOE.

Exhaustive: Used to describe the conduct of an analysis or other activity; related to systematic but considerably stronger in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan but also that the plan followed is sufficient to ensure that all possible avenues have been exercised.

Explicit Requirements: Functional security requirements or security assurance requirements specified in a PP or ST that satisfy a specific consumer need but do not originate from the CC catalog of standardized components (*see also* Refinement and Extended).

Extended: Addition to an ST or PP of requirements not contained in Part 2 or assurance requirements not contained in Part 3 of the CC; extensibility (*see also* Explicit requirements and Refinement).

External IT Entity: Any IT product or system, distrusted, or trusted, outside of the TOE that interacts with the TOE.

F

Family: Grouping of security requirements that share security objectives but may differ in emphasis or rigor; the members of a family are termed components.

Federally-Funded Research and Development Centers: Members of various FFRDCs are used as validators in the U.S. scheme.

Formal: Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

G

Governance: Used as the tag for stakeholder class of individuals who help develop guidance and policy over IA relevant software.

H

Hierarchy: Ordering of components within a family to represent increasing strength or capability of security requirements that share a common purpose; on occasion, partial ordering is used to illustrate the relationship between nonhierarchical sets.

I

Information Assurance: Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information System: a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Since information systems can comprise multiple products, different C&A schemes for products and systems can sometimes conflict with one another.

Information Technology Product: Package of IT hardware, software, and firmware that provides functionality designed for use or incorporation within a multiplicity of systems. An IT product can be a single product or multiple IT products configured as an IT system, network, or solution to meet specific customer needs. In either case, the testing occurs in a testing facility or a client's site under laboratory conditions, and not in the actual operational environment.

Information Technology Security: All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

Information Technology Security Evaluation Criteria: a compilation of the information that must be provided and of the actions that must be taken in order to give grounds for the confidence that evaluations will be carried out effectively and to a consistent standard throughout an evaluation and certification/validation scheme.

Information Technology Security Evaluation Facility: an accredited EF, licensed or approved to perform evaluations within the context of a particular IT security evaluation and certification/validation scheme.

Information Technology Security Evaluation Methods: Compilation of the methods that need to be used by Evaluation Facilities in applying ITSEC in order to give grounds for confidence that evaluations will be carried out effectively and to a consistent standard throughout an evaluation and certification/validation scheme.

Information Technology Security Policy: Rules, directives, and practices that govern how assets, including sensitive information, are managed, protected, and distributed within an organization and its IT systems.

Input task: Tasks related to the management of all required, sponsor-supplied evaluation evidence.

Integrity: Prevention of unauthorized modification of information.

Internal communication channel: Communication channel among different parts of a TOE.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.

Inter-TSF transfers: Communicating data between the TOE and the security functions of other trusted IT products.

Iteration: Use of an element more than once with varying parameters.

J

Justification: Analysis leading to a conclusion but which is more rigorous than a demonstration; requires significant rigor in terms of very carefully and thoroughly explaining every step of a logical argument.

M

Monitoring of Evaluations: Procedure by which representatives of a CB observe in progress or review completed evaluations in order to satisfy themselves that an ITSEF is carrying out its functions in a proper and professional manner.

Monitoring Phase: Middle of an assurance maintenance cycle during which the developer provides evidence at one or more points that assurance of the TOE is being maintained in accordance with established plans and procedures; this evidence is independently validated by an evaluator.

N

National Security Information: information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure.

National Security Systems: any telecommunications or information system operated by the United States Government, the function, operation, or use of which—

a. involves intelligence activities;

b. involves cryptologic activities related to national security;

c. involves command and control of military forces;

d. involves equipment that is an integral part of a weapon or weapons system; or

e. subject to subsection (b[31]), is critical to the direct fulfillment of military or intelligence missions.

(see section C.2 for context)

National Voluntary Laboratory Accreditation Program: the U.S. accreditation authority for CCTLs operating within the NIAP CCEVS.

Network Security: Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

---

[31] (b) LIMITATION – Subsection (a)(5) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

NIAP Validation Body: A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the CCEVS.

O

Object: Passive entity within the TOE security function (TSF) scope of control (TSC) that contains or receives information and upon which subjects perform operations.

Observation Decision: A response to an Observation Report (OR). The observation decision (OD) is the formal documented response from the Validation Body that provides clarification/guidance to the CCTL on a submitted OR.

Observation Report: A report issued to the NIAP Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Operations Security: the implementation of standardized operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to (1) maintain a system in a known secure state at all times, and (2) prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources.

Organizational Security Policy: one or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Output Task: Tasks related to the reporting of information through either an Observation Report or Evaluation Technical Report.

P

Package: Set of either functional or assurance components (e.g., an EAL), combined together to satisfy a subset of identified security objectives; packages are intended to be used to build PPs and STs.

Preventive Security Objective: Security objectives that prevent a threat from being carried out or limit the ways in which it can be carried out.

Principal Security Assurance Requirement: Security assurance requirement that directly contributes to assuring that an entity meets its security objectives.

Principal Security Functional Requirement: Security functional requirement that directly satisfies the identified security objectives of the TOE.

Procedures: step-by-step "how to" tasks which are necessary to conduct a process and meet standards.

Process: Used as the tag for stakeholder class of individuals who help develop or manage the current NIAP process.

Producer: Used as the tag for stakeholder class of individuals who help develop IA relevant software.

Product: a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Profile: Structure that characterizes the behavior of users and subjects; it represents how users and subjects interact with the TSF.

Profile Metrics: Ways in which various types of user and subject activities are recorded and measured in a profile; serves as input to pattern recognition.

Profile Target Group: One or more users who interact with the TSF, supposedly according to historical patterns or patterns of expected behavior.

Protected Information: Information gathered or obtained during an evaluation, the unauthorized disclosure of which could reasonably be expected to cause: (1) harm to competitive commercial or proprietary interests, (2) a clearly unwarranted invasion of personal privacy, (3) damage to national security, or (4) harm to an interest protected by national law, legislation, regulation, policy, or official obligation.

Protection Profile: (1) Formal document defined in the CC that expresses an implementation-independent set of security requirements for an IT product that meets specific consumer needs. (2) Complete combinations of security objectives and functional and assurance requirements with associated rationale.

Protocol: a set of semantic and syntactic rules that determine the behavior of entities that interact.

Prove: Formal analysis in the mathematical sense, which is completely rigorous in all ways.

R

Recognition of Common Criteria Certificates: Acknowledgment that the evaluation and certification processes carried out by compliant CBs appear to have been carried out in a duly professional manner and meet all the conditions of the CCRA and the intention to give all resulting CC Certificates equal weight.

Reevaluation: Evaluation of a new version of the TOE that addresses all security-relevant changes made to the certified version of the TOE and reuses previous evaluation results where they are still valid.

Reevaluation Phase: Completion of the assurance maintenance cycle in which an updated version of the TOE is submitted for reevaluation based on changes affecting the TOE since the certified version.

Reference Monitor: Concept of an abstract machine that enforces TOE access control policies.

Reference Validation Mechanism: Implementation of the reference monitor concept that possesses the following properties: tamper-proof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement: Addition of extra details to an element when it is used in a PP or ST (*see also* Explicit requirement and Extended).

Reliability: Property of consistent intended behavior and results.

Request for Interpretation: submitted by evaluation authorities to CCIMB; the four types are (1) perceived error such that some content in the CC or CEM requires correction, (2) identified need for some additional material in the CC or CEM, (3) proposed method for applying the CC or CEM in a specific circumstance for which endorsement is sought, and (4) request for information to assist with understanding the CC or CEM.

Residual Risk: (1) Portion of risks remaining after security measures has been applied. (2) Risk that remains after safeguards have been implemented.

Revocation: Removal of the accredited status of a laboratory if the laboratory is found to have violated the terms of its accreditation.

Rigor: Degree of structure and formality applied to the evaluation by the evaluators.

Risk: (1) Combination of the likelihood that a threat will be carried out and the severity of the consequences should it happens. (2) Potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Risk Assessment: (1) Process of analyzing threats to and vulnerabilities of an IT system and the potential impact the loss of information or capabilities of a system would have; the resulting analysis is used as the basis for identifying appropriate and cost-effective countermeasures. (2) Process of identifying security risks, determining their magnitude, and identifying areas requiring safeguards.

Risk Management: (1) Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected. (2) The entire process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources.

Role: Predefined set of rules establishing the allowed interactions between a user and the TOE.

S

Safeguard: Practice, procedure, or mechanism that reduces risk.

Scope of Accreditation: Approved test methods for which a CCTL has been accredited.

Scope: Portion of an IT product or system that is being evaluated.

Security Assurance: Grounds for confidence that an entity meets its security objectives.

Security Attribute: Information associated with users, subjects, and objects used for the enforcement of the TSP.

Security Classification: Labeling applied to protected information to indicate minimum standards of protection that need to be applied in the national or organizational interest; also referred to as protective marking.

Security Flaw: Condition that alone or in concert with others provides an exploitable vulnerability. TSP violations that occur not from a problem with the hardware, software, or firmware portion of a TOE but from a problem in the TOE guidance are also recognized as security flaws.

Security Objective: Statement of intent to counter identified threats and/or satisfy identified organization policies and assumptions.

Security Target: A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the CC. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Selection: Specification of one or more items that are to be selected from a list given in the element definition.

Semiformal: Expressed in a restricted syntax language with defined semantics.

Sensitive Information: Any information for which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or conduct of federal programs or the privacy to which individuals are entitled under the Privacy Act Section 552a of Title 5 USC, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Security Function: Part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Software Assurance: The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures.

Sponsor: The person or organization that requests a security evaluation of an IT product or protection profile.

Standards: documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics to ensure that materials, products, processes, and services are fit for their purpose.

Strength of Function: a qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

Strength of Function-Basic: Level of the TOE strength of function where analysis shows that the function provides adequate protection against causal breach of the TOE security by attackers possessing a low attack potential.

Strength of Function-High: Level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of the TOE security by attackers possessing a high attack potential.

Strength of Function-Medium: Level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of the TOE security by attackers possessing a moderate attack potential.

Subactivity: Application of a CC assurance component.

Subject: Active entity within the TSC that causes operations to be performed.

Subtask: Subdivision of a task.

Supporting Security Assurance Requirement: Security assurance requirement that indirectly contributes to assuring that an entity meets its security objectives.

Supporting Security Functional Requirement: Security functional requirement that does not directly satisfy security objectives for the TOE but which provides support to the principal SFRs and hence indirectly helps satisfy TOE security objectives.

System Integrity: Property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system.

T

Target of Evaluation: An IT product, part of an IT product or group of IT products and associated documentation that is the subject of a security evaluation under the CC.

Target of Evaluation Guidance: Administrator guidance, user guidance, flaw remediation guidance, delivery procedures, and installation, generation, and start-up procedures.

Target of Evaluation Security Functions; a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

Target of Evaluation Security Functions Scope of Control: the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

Target of Evaluation Security Functions Interface: the set of interfaces, whether interactive man-machine interfaces or application program interfaces, through which resources are accessed that are mediated by the TSF or information obtained from the TSF.

Target of Evaluation Security Policy: a set of rules that regulate how assets are managed, protected, and distributed within a TOE.

Target of Evaluation User: Focal point in the user organization that is responsible for receiving and implementing fixes to security flaws. This is not necessarily an individual user but may be an organizational representative who is responsible for the handling of security flaws.

Task: Specifically required CEM evaluation work that is not derived directly from a CC requirement.

Test Method: An evaluation assurance package from the CC, the associated evaluation methodology for that assurance package from the CEM, and any technology-specific derived testing requirements.

Threat: (1) Any circumstance or event with the potential to harm an IT system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (2) Potential danger that a vulnerability may be exploited intentionally,

triggered accidentally, or otherwise exercised. (3) A potential cause of an unwanted incident, which may result in harm to a system or organization.

Trusted Channel: Means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted Path: Means by which a user and a TSF can communicate with necessary confidence to support the TSP.

U

Users: ISO/IEC recognizes two types of authorized users: (1) local or remote human users, and (2) external IT entities. Users are considered to be outside a TOE and interact with a TOE through the TSFI.

V

Validation: The process carried out by the NIAP Validation Body leading to the issue of a CC certificate.

Validated Products List: A publicly available document issued periodically by the NIAP Validation Body giving brief particulars of every IT product or protection profile which holds a currently valid CC certificate awarded by that body and every product or profile validated or certified under the authority of another Party for which the certificate has been recognized.

Validation Report: A publicly available document issued by the National Evaluation Authority (in the U.S. the NIAP Validation Body which summarizes the results of an evaluation and confirms the overall results, (i.e., that the evaluation has been properly carried out, that the CC, the Common Evaluation Methodology, and scheme-specific procedures have been correctly applied; and that the conclusions of the Evaluation Technical Report are consistent with the evidence adduced).

Verification: (1) Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled. (2) Process of comparing two levels of an IT system specification for proper correspondence, such as security policy model with top-level specification, top-level specification with source code, source code with object code.

Verify: Independent evaluator actions; similar to *confirm* but more rigorous.

Vulnerability: Weakness in the design, operation, or operational environment of an IT system or product that can be exploited to violate the intended behavior of the system relative to safety, security, and/or integrity.

W

Work Units: Smallest unit of an evaluation action; derived from an evaluator action element or a content and presentation of evidence element.

C.2 Some context for terminology used in this report

C.2.1 Cybersecurity and Related Terms

In this report, the terms *cybersecurity* and *information assurance* are used interchangeably. *Cybersecurity* emerged concurrently with DHS. It is used in *The Strategy to Secure Cyberspace* and gained formal status when The Department of Homeland Security Authorization Act for Fiscal Year 2005 [DHS2005] amended the Paperwork Reduction Act to define it as:

> the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Whereas *cybersecurity* is the preferred term of DHS, *information assurance* is the preferred term of the defense and intelligence communities, where it has been well-defined for a long time. The definitions given in the *National Information Systems Security (INFOSEC) Glossary* [NST2000c], *Information Assurance (IA) Awareness Program*, (AFI33- 204), and the Industry Advisory Council, Shared Interest Group on Information Assurance are all similar:

> conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Both *cybersecurity* and *information assurance* encompass the "five pillars" of information assurance – availability, integrity, authentication, confidentiality, and nonrepudiation of information systems – as well as the concepts of protection and restoration. *Cybersecurity* refers explicitly to computers and electronic systems, whereas *information assurance* refers more broadly to information systems, which might or might not be electronic.

Information security is often erroneously equated with i*nformation assurance*. Unlike *information assurance*, *information security* is not well-defined by anyone [PETERSEN2004]. In fact, the authoritative source of information systems security terminology, the *National Information Systems Security (INFOSEC) Glossary* [NST2000c] doesn't define the term *information security*, preferring the terms *information assurance*, *computer security,* and *information systems security (INFOSEC or ISS)*. It defines *computer security* as:

> measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

The term *computer security* dates from a more centralized, single-system approach in contrast to the networked, distributed systems of today. With the growth of the Internet

especially, the term *network security* has become more widely used. [NST2000c] equates *network security* to *INFOSEC/ISS* and defines them as:

> protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

INFOSEC/ISS does not encompass the five pillars, nor does it refer to restoration of services. For these reasons and to minimize confusion, this report prefers the terms *cybersecurity* and *information assurance* to all these other terms.

C.2.2 National Security Systems

Another term of significance to this report is *national security systems* (NSS). This is because the security requirements of NSSs are more stringent than those of other information systems. Section 5142 of the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) [CCA1996] first defined *national security systems* as:

> any telecommunications or information system operated by the United States Government, the function, operation, or use of which—
>
> 1. involves intelligence activities;
> 2. involves cryptologic activities related to national security;
> 3. involves command and control of military forces;
> 4. involves equipment that is an integral part of a weapon or weapons system; or
> 5. subject to subsection (b32), is critical to the direct fulfillment of military or intelligence missions.

C.2.3 Critical Infrastructure Protection

Several recent Government Accountability Office (GAO) reports [GAO2004c and GAO2004f] have underscored the vulnerability of the *critical infrastructure* to cybersecurity threats. The *critical infrastructure* is defined by numerous sources ([ATIS2000], [EO13010], [NST2000c], [WH2003]) as:

> banking and finance, energy, chemical sites, transportation, telecommunications, Government facilities, dams, national monuments and icons. *Cybersecurity* is a key element of infrastructure protection.

Although most critical infrastructures are in the private sector, governments at all levels perform key functions that depend on information networks, systems, and products.

---

[32] (b) LIMITATION – Subsection (a)(5) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

While *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, [WH2003] addressed physical security of the critical infrastructure, *The National Strategy to Secure Cyberspace* [WH2003a] addressed the protection of cyberspace. One of the priorities that it identifies is the need for a National Cyberspace Security Threat and Vulnerability Program. This would be a coordinated effort between governments and the private sector to identify and remediate the most serious cyber vulnerabilities through collaborative activities, such as sharing best practices and evaluating and implementing new technologies. The NIAP is an integral part of this and another strategy priority, that of securing governments' cyberspace.

The terms *cyberspace*, *cybersecurity*, *cyberwarfare*, and *cyberterrorism* do not appear in [NST2000c], having entered the lexicon since September 11. The National Infrastructure Protection Center (NIPC) under Director Ron Dick [BERINATO2002] defined *cyberterrorism* as:

> a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.

As documented by the GAO, several sources point to an escalation in the cyberterrorism threat. The Federal Bureau of Investigation (FBI) identifies the following *threats* to the critical infrastructure: criminal groups, foreign intelligence services, hackers, hactivists, information warfare, insiders, and virus writers. Experts agree that there has been a steady advance in the level of sophistication and effectiveness of attack technology.

C.2.4 Quality-related Terms

From 1995 through 2003, the CERT® Coordination Center reported 12,946 security vulnerabilities that resulted from software flaws. This is significant because the potential for attack increases when a product has software flaws. *Software assurance* methods evaluate products for flaws. The Institute of Electrical and Electronics Engineers (IEEE) Standard Glossary of Software Engineering Terminology [IEEE2002] defines *software assurance* as:

> the planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures.

As an example, Title III of the E-Government Act (Public Law 107-347), entitled the Federal Information Security Management Act (FISMA), requires NIST to develop risk-based minimum information security *standards* for systems other than those dealing with national security. However, there is often confusion regarding the terms standards, guidelines, best practices, procedures, and protocols.

The International Organization for Standardization (ISO) [ISO1996a] defines *standards* as:

> documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions

> of characteristics to ensure that materials, products, processes, and services are fit for their purpose.

As a recent document on cybersecurity Practices and Standards Guidance [CIDX2004] notes, differentiating between a *standard* and a *guideline* can be difficult. It says:

> Unfortunately, no litmus test can be applied to determine when a guideline may actually be a standard. The name assigned to the document or meeting may be of little consequence. It is the degree to which the material details a prescribed set of rules for procedures, specifications, materials, design, performance or operation (whether voluntary or mandatory) that is critical in determining if an industry standard has been established.
>
> While both standards and guidelines are usually voluntary, standards are more susceptible to use by others as evidence of a minimum level of care, despite disclaimers to the contrary.

According to the GAO [GAO1997], *best practices* refer to the:

> processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency.

The Sacramento County Office of Quality and Strategic Planning [QUALITYn.d.] defines *procedures* as:

> step-by-step "how to" tasks which are necessary to conduct a process and meet standards.

The IEEE Portable Applications Standards Committee [IEEE1995] defines *protocol* as:

> a set of semantic and syntactic rules that determine the behavior of entities that interact.

C.2.5 Certification and Accreditation

Many Federal agencies are using certification and accreditation (C&A) is to ensure that products and systems are secure. In addition to requiring NIST to develop security standards, FISMA also requires C&A of *information systems*.

ISO defines *certification* as:

> the procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements or standards.

ISO defines *accreditation* as:

> the procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks. In the context of

> certification, an accreditation body might accredit a certification body, such as a testing laboratory, as competent to carry out certification activities—in a sense, certifying the certifiers.

C&A can either be *product*- or *information system*-specific. The CC defines a *product* as:

> a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Various sources [Title 44 U.S.C., Section 3502 and OMB1996] define an *information system* as:

> a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Since information systems can comprise multiple products, different C&A schemes for products and systems can sometimes conflict with one another.

C.2.5.1 Product C&A

Although C&A is applied to product evaluations, for the purposes of this report, product or algorithm evaluation will be the preferred term when referring to evaluations below the system level. The NSTISSP 11 [NST2002; NST2003] policy directs departments and agencies of the U.S. Federal Government to acquire only COTS IA and IA-enabled IT *products* (to be used on systems entering, processing, storing, displaying, or transmitting *national security* information) that have been evaluated and validated in accordance with criteria, schemes, or programs of the:

1. ISO/IEC15408, Common Criteria,
2. The NIAP evaluation and validation program, and
3. FIPS validation program. [NST2003].

To avoid having two different standards, one for national security systems and one for the rest of the systems in DoD, DoD Directive (DoDD) 8500.1 [DoD2002a] requires ***all*** DoD systems to meet NSTISSP 11 requirements.

The rest of the Federal Government is not required to evaluate and validate the products they use.

C.2.5.2 Information System C&A

Although C&A is applied to product evaluations, for the purposes of this report, C&A will be the preferred term when referring to evaluations at the system level. To address *information system*-level security concerns, four C&A processes have emerged:

1. DoD Information Technology Security Certification and Accreditation Process (DITSCAP) [DoD1997], which applies to all DoD entities;

2. National Information Assurance Certification and Accreditation Process (NIACAP), which applies to National Security Systems;
3. Protecting Sensitive Compartmented Information Within Information Systems, Director of Central Intelligence Directive 6/3 (DCID 6/3), which applies to the Intelligence Community; and
4. Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication SP 800-37, which applies to all U.S. Government Executive Branch departments, agencies, and their contractors and consultants.

The first three are mandatory for their communities, while the NIST SP provides *guidelines* for certifying and accrediting information systems supporting the executive agencies of the Federal government.

DITSCAP, upon which NIACAP is based, was developed first. It is a four-stage process:

- Phase I - Definition – Defining and documenting mission, function, requirements, and capabilities, culminating in a draft system security authorization agreement (SSAA);
- Phase II - Verification – Verifying the evolving or modified system's compliance with the SSAA;
- Phase III - Validation – Validating the SSAA using vulnerability and penetration testing, resulting in full, interim, or withheld accreditation;
- Phase IV - Post accreditation – Monitoring and maintenance to ensure continued security.

The goal of these processes is to introduce integrated security into the life cycle of IT systems to minimize risks in shared infrastructures. Both DITSCAP and NIACAP define *certification* as:

> The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Their shared definition of *accreditation* is:

> Formal declaration by the Designated Accrediting Authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

As part of its FISMA Implementation Process, NIST developed SP 800-37 [NIST2002b]. Its definitions of C&A are almost identical to those of DITSCAP and NIACAP:

> *Certification*: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
>
> *Accreditation*: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

In keeping with FISMA requirements, the NIST, DITSCAP, and NIACAP definitions of accreditation emphasize the concept of risk, which the ISO definition does not.

Annex E Policy

This annex contains a detailed discussion of the policies and other documents relating to the NIAP. The policies are grouped in roughly hierarchical order based on the five themes of cybersecurity, Standards/Guidelines, Education and Training, Research, and Acquisition. Certain documents may appear multiple times to account for multiple themes within these documents. The detailed description of each theme is contained within Chapter 3, but a short summary will precede the documents so that the reader need not go back and forth between the chapter and this appendix. The Tab A at this end of this Annex provides a broad overview of the policies and the thematic areas covered, and illustrate the complexity of the policy landscape.

D.1 Cybersecurity

The first theme is cybersecurity. This word is frequently used interchangeably with information security and information assurance. It is a component of the critical infrastructure. This theme will, therefore, address the policies surrounding cybersecurity as part of the critical infrastructure. The grouping that follows reflects the explicit relationships among the policies.

D.1.1 Computer Security Act (CSA) 1987[33]

The CSA was Congress's first attempt to specify actions the Federal government needed to take to address a real and growing problem. It states the goal of Congress is to improve the security and privacy of sensitive information in Federal computer systems. Congress directed the following actions: (1) assigned NIST the responsibility for developing standards and guidelines (spelled out in detailed later on in this section) with advice from NSA where appropriate; (2) provided a mechanism for promulgation of these standards and guidelines, including specifying which are mandatory and which are voluntary; (3) required establishment of security plans for Federal computer systems that contain sensitive information; and (4) required mandatory periodic training for all personnel involved in management, use, or operation of Federal computer systems that contain sensitive information.[34] The documents that follow in this section were issued primarily in response to the requirements laid out by this statute.

D.1.2 National Security Directive 42[35] 1990 (NSD 42)

NSD 42 established policy and procedures intended to ensure that information housed in National Security Systems (NSS) cannot be exploited for hostile purposes. The specific policy states that:

> a. U.S. Government (USG) national security systems shall be secured by such means as are necessary to prevent compromises, denials or exploitation;

---

[33] Public Law 100-235, 40 USC 759, "Computer Security Act of 1987."

[34] Ibid, Section 2.

[35] National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," 5 July 1990.

b. Federal agencies shall require that national security systems operated and maintained by U.S. Government contractors likewise be secured.[36]

This document defined NSS for the first time as those telecommunications and information systems operated by the USG, its contractors or agents, that contain classified information or involve intelligence activities related to national security, command and control of military forces, equipment integral part of a weapon or weapon system, or equipment critical to the direct fulfillment of military or intelligence missions. It created an organizational structure to guide efforts to secure NSS from exploitation, establishes a mechanism to develop and disseminate policy, and assigns roles and responsibilities for implementation. The National Security Council/Policy Coordinating Committee (NSC/PCC) for the National Security Telecommunications and Information Systems was assigned responsibility for overseeing implementation of NSD-42 and for developing policy recommendations and providing guidance to the National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISSC, later renamed the Committee for National Security Systems (CNSS) by Executive Order 13231, in turn, was charged with developing operating policies, procedures, guidelines, instructions and standards to implement NSD-42. One of this Directive's stated objectives is the creation of "a technical base within the U.S. Government to achieve this security, and initiatives with the private sector to maintain, complement, or enhance that government technical base and to ensure information systems security products are available to secure NSS."[37]

D.1.3 NSTISSC/CNSS Issuances

The Secretary of Defense (SECDEF) is designated as the Executive Agent for National Security Systems. The Director, NSA (DIRNSA) is designated as the National Manager for National Security Systems and is responsible for the permanent secretariat for the Committee for National Security Systems (formerly the NSTISSC).[38] Through the CNSS Issuances (instructions, directives, manuals and advisory memoranda), SECDEF and the National Manager provide policy and guidance to on cybersecurity to Federal agencies who are members of the NSS. A complete list of these issuances can be found at the following web site: http://www.nstissc.gov/html/library.html.

D.1.4 Executive Order 12333[39] of 1981 (EO 12333)

This document provided policy and guidance to the intelligence community (IC) and spelled out responsibilities of the various entities within this community as well as identifying what Federal components are considered to be part of this community. Additionally, it designated the Director of Central Intelligence (DCI) as the head of this community and gave that position the authority to provide policy and guidance to the IC, including common security and access standards for managing and handling foreign intelligence systems, information and products.

---

[36] Ibid, para 2.

[37] NSD 42, para 1.b.

[38] NSD 42.

[39] EO 12333, "United States Intelligence Activities," 4 December 1981.

D.1.5 Executive Order 12958[40] of 1995 (EO 12958)

This order prescribed a "uniform system for classifying, safeguarding and declassifying national security information." It provided definitions for national security and classified national security and instructions on classification/declassification standards and authorities. It also directed agency heads to establish uniform procedures to ensure that Information Technology (IT) systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process or store classified information have controls that (1) prevent access by unauthorized persons, and (2) ensure the integrity of the information.

D.1.6 Executive Order 13010 Critical Infrastructure Protection[41] of 1996 (EO 13010)/Presidential Decision Directive 63 1998 (PDD 63)

These two documents were the seminal documents in the Administration's efforts to define and address the issue of Critical Infrastructure Protection. EO 13010 was the original executive order chartering the President's Commission on Critical Infrastructure Protection to assess "the scope and nature of the vulnerabilities of, and threats to, critical infrastructures"[42] and make recommendations on what the Administration should do about the issue. The EO also established the Infrastructure Protection Task Force within the Department of Justice to handle coordination of existing infrastructure protection efforts until the Commission made its recommendations. The Commission issued its report in 1997, where it identified a number of sectors, including the information and communications sector, and described vulnerabilities, findings and recommendations.[43]

The Clinton Administration's response to the recommendations of the Commission was the issuance of Presidential Decision Directive 63[44] (PDD 63). This document defined, for the first time, the critical infrastructure, lead agencies and expectations of the private sector and government to begin to address the risks posed to U.S. critical infrastructures. The Department of Commerce was designated the lead agency for the Information and Communications Sector. For the Federal government, it stated that department and agencies were responsible for protecting their own critical infrastructures, especially their *cyber-based* systems. It called for vulnerability assessments on government computer and physical systems and for departments and agencies to develop plans for protecting their critical infrastructures, including their *cyber-based systems.* The plans were to be implemented no later than two years from the date of the document and updated every two years. This document also set up a number of new entities: the National Infrastructure Protection Center (NIPC) at the FBI; Information Sharing and Analysis Centers (ISAC) set up by sector coordinators with the private sector; and a number of follow-on studies. It also created the position of a National Coordinator who reported to

---

[40] EO 12958, "Classified National Security Information," 17 April 1995.

[41] EO 13010, "Critical Infrastructure Protection," 15 July 1996.

[42] Ibid, Sec 4 Mission.

[43] PCCIP, *Critical Foundations: Protecting America's Infrastructures,* October 1997, Appendix A "Sector Summary Reports, pp. A-2–A-10.

[44] PDD63, "Critical Infrastructure Protection," 22 May 1998.

the President through the Assistant to the President for National Security Affairs.[45] The significance of this activity to the NIAP was that, for the first time, cybersecurity was identified as an issue of concern to the Federal government and the process to evaluate software embodied in the NIAP process is an essential element contributing to cybersecurity.

D.1.7 Executive Order 13231[46] of 2001(EO 13231)

This document sets policy for protecting information systems for critical infrastructures. It states that:

> It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

This EO also renamed NSTISSC to the CNSS, but left its chairmanship and charter intact. It established a Critical Infrastructure Protection Board (CIP Board) chaired by the President's Special Advisor for Cyberspace Security. This board chartered a number of standing committees, as well as incorporating two existing committees, one of which was the CNSS.[47] The public-private partnership called out in this EO is a partnership between the government and private sector owners/operators of the critical infrastructures.[48].

D.1.8 Paperwork Reduction Act of 1980 as amended by the Paperwork Reduction Act of 1995 (PRA)[49]

The purpose of this statute was a nearly complete revision of the original PRA of 1980 to provide comprehensive direction to the Federal government to become more responsive and accountable for reducing the burden of Federal paperwork on the public. It also addressed a number of other information management policies, including ensuring that the creation, collection, maintenance, use, dissemination, and disposition of information for or by the Federal government is consistent with applicable laws relating to the security of information, including CSA 1987. The Act created an Office of Information and Regulatory Affairs in OMB whose head was responsible for accomplishing those

---

[45] Although this position still exists, the majorities of the functions were assigned to the Department of Homeland Security by the HSA 2002 and are performed in the National Cyber Security Division (NCSD) of the Directorate for Information Analysis and Infrastructure Protection.

[46] EO 13231, "Critical Infrastructure in the Information Age," 18 Oct 2001.

[47] ibid, Sections 2 & 7.

[48] This board, along with the standing committees it established, was disestablished by a later EO. The two preexisting committees, CNSS and NCS's Committee of Principles (COP), remained in existence under their original charters. EO 13284, "Amendment of Executive Orders, and other Actions, in Connection With the Establishment of the Department of Homeland Security," 23 January 2003, Section 2.

[49] Public Law 104-13, "Paperwork Reduction Act of 1995," 22 May 1995 (44 USC Chapter 35).

oversight activities assigned to the Director, OMB, for information resources. These activities include development, coordination and oversight of the implementation of Federal information resources management policies, principles, standards and guidelines, for, among other things, the security of information. Federal agencies were responsible for carrying out the agency's information resources management activities to improve agency productivity, efficiency and effectiveness and agency heads were directed to designate a senior official to carry out these responsibilities. This position in later statutes became the CIO. Agencies were also directed to implement and enforce policies, procedures, standards, and guidelines on security for the agencies and to identify and to apply appropriate security measures as indicated by their risk management assessment consistent with CSA 1987.

D.1.9 Clinger-Cohen Act 1996(CCA)[50]

This statute (originally titled "Information Technology Management Reform Act") was a significant effort on the part of Congress to make substantial changes in how the Federal government acquired and managed information technology.[51] The CCA gave the Office of Management and Budget (OMB) authority over the Federal agencies IT programs and required: the establishment of a capital planning process; use of performance and results-based management; designation of federal agency Chief Information Officers (CIOs); and a number of annual reports on progress in implementing the statute.

The CCA directed agency CIOs to establish an IT capital planning process, of which information security is a component, and modified the requirement to develop and implement information security plans, originally required by CSA1987, by providing more details on what should be included in the plan. Additionally, it reiterated the direction to the Secretary of Commerce to issue standards and guidance on information security (developed by NIST) originally required by CSA 1987, and included the determination of which standards should be made mandatory and which should be made voluntary. It gave the Federal agency heads the authority to employ more stringent standards and a waiver process for those standards determined by the Secretary of Commerce to be mandatory standards. The statute also defined national security systems in law for the first time and specified what part of the act applied to these systems. Finally, the CCA directed OMB to evaluate Federal agency programs in information technology management and, in particular, to ensure that agency information security policies, procedures and practices were adequate.

---

[50] Public Law 104-106, Division E, "Information Technology Management Control Act of 1996," 10 Feb 1996, sections 5113, 5131, 5141, 5142, and 5607.

[51] H.R. Report 104-450 to accompany S.1124, Division E- "Information Technology Management Reform", pages 972-982 discusses Congress's frustration with the lack of progress within the Federal government in the area of information technology and their intent in giving the Director, OMB, significant oversight authority in establishing performance-based and results-based management for IT.

D.1.10 Executive Order 13011 (EO 13011)[52]

This EO was issued to provide policy direction to Federal agencies to assist their implementation of the requirements to improve the acquisition and management of information technology as required by CCA and the Paperwork Reduction Act of 1995 (PRA). The EO laid out the administration's policy regarding the management of Federal IT systems; defined the responsibilities of agency heads; chartered the Chief Information Officer's Council, the Government Information Technology Services Board, and the Information Technology Resources Board (including membership & responsibilities), and specific responsibilities of designated offices for this policy. It reiterated agency head responsibilities for ensuring that their information security policies, procedures and practices were adequate and provided additional clarification of what constituted a national security system. This EO also directed OMB to provide to the Federal agencies, implementation guidance for this EO and on the management of information resources.

D.1.11 Office of Management & Budget Circular A-130 (OMB Cir A-130), Revised, Transmittal Memorandum No. 4, 28 November 2000[53]

As directed by EO 13011, OMB issued this Circular to provide implementing policy to Federal agencies for several statutes, including the PRA, CCA and the CSA. To ensure security in information systems as required by the three statutes cited, OMB directed agencies to incorporate security into the architecture of their information and systems, and fund and manage security through plans built into the life-cycle budgets for information systems. This document also laid out responsibilities for all Federal agencies, as well as specific responsibilities for certain government agencies (such as DoD, Government Services Administration (GSA), and the National Archives and Records Administration (NARA)), as well as OMB's role in ensuring information security for Federal systems. To accomplish these objectives, OMB provided detailed guidance in Appendix III of this circular.[54] As described, agencies must ensure that information was protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. Within their IT capital planning process, agencies were required to establish oversight mechanisms to evaluate and ensure the continued security of their systems and data. As part of this, agencies must develop a security plan, based on criteria specified in this appendix.

D.1 12 DoD Issuances

The authorities of the Director, OMB, described above, are delegated to SECDEF in the case of systems operated by DoD, contractors for DoD or another entity on behalf of DoD that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of

---

[52] Executive Order 13011, "Federal Information Technology," 16 July 1996.

[53] OMB Circular A-130, "Management of Federal Information Resources," Revised, transmittal No. 4, 20 November 2000.

[54] Appendix III, OMB Circular A-130,"Security of Federal Automated Information Resources," November 2000.

DoD.[55] DoD has been very active in providing policy to its subordinate organizations. The primary document for cybersecurity (information assurance in DoD's terminology) is DoD Directive 8500.1.[56] This document describes the overall DoD policy for this area and assigns responsibility for execution of the program to the DoD CIO. The companion instruction, DoD Instruction 8500.2 provides details for the execution of the programs.[57] A lower level document, Chairman of the Joint Chiefs of Staff Instruction 6510.01D describes the IA program for the Joint Staff, combatant commands and military services.[58] There are other documents that contain policy for the Department in specific areas, but these three are the major ones outlining the entire IA program.

D.1.13 Intelligence Community

As this document was being written, the leadership of the Intelligence Community (IC) was undergoing significant change in light of the post-9-11 concerns about intelligence reform. It is outside the scope of this study to present an in-depth assessment of the on-going changes that are occurring. For the purposes of this study, discussion is limited to four documents that establish the responsibilities for oversight of the community IT and cybersecurity. The four documents include:

D.1.13.1 National Security Act of 1947 (NSA 1947)

D.1.13.2 EO12333, United States Intelligence Activities 1981

D.1.13.3 EO 13355, Strengthened Management of the Intelligence Community, 2004

D.1.13.4 Intelligence Reform and Terrorism Prevent Act 2004 (IRTPA 2004)

These four documents described the existence, organization and management of the Intelligence Community. As directed in the National Security Act of 1947[59] and reinforced by EOs12333,[60] and 13355,[61] the DCI has oversight of the Intelligence Community and authority to develop policies, procedures and standards for activities of the Federal agencies that fall within the IC. This is separate and above the DCI's responsibilities for the CIA, similar to SECDEF's executive agent responsibility for NSS. The most recent document, IRTPA 2005, designated the Director of National Intelligence (DNI) as the head of the intelligence community with the authority to "…establish

---

[55] 40 USC subsection 3543, para (b)(2)

[56] DoDD 8500.1, "Information Assurance," 24 October 2002.

[57] DoDI 8500.2, "Information Assurance Implementation," 6 February 2003.

[58] CJCSI 6510.01D, "Information Assurance and Computer Network Defense," 15 June 2004.

[59] National Security Act of 1947, as amended, 26 July 1947, "Responsibilities of the Director of Central Intelligence," Sections 103-104.

[60] EO 12333, "United States Intelligence Activities," para 1.5, "Director of Central Intelligence," 4 December 1981.

[61] EO 13355, "Strengthened Management of the Intelligence Community," Section 2, (b), 27 August 2004.

uniform security standards and procedures; and establish common information technology standards protocols, and interfaces…."[62]

D.1.14 OMB Memo M-00-07, 28 Feb 2000[63]

OMB issued this memo to provide guidance to Federal agencies concerning incorporating and funding security as part of the agency information technology systems and architectures. It also provided the criteria that would be used to evaluate security for information systems, as required by CCA 1996. As the revision to OMB Circular A-130 addressing these details had yet to be issued (in transmittal No. 4 described previously), this memo was a heads-up to the Federal agencies on what they should be preparing to accomplish and reminded them of the responsibilities detailed in not only CCA, but also CSA, PRA, and the previous version of the OMB Circular A-130. Specifically, the memo outlined the principles and policy for information security of Federal systems, including consistency with security guidance issued by NIST. It also stated that security for national security systems would be implemented in accordance with appropriate national security directives.

D.1.15 Government Information Security Reform (GISR) 2001[64]

This act was the first major revision of Federal information security requirements since CCA. The statute created a new subchapter of title 44 U.S. Code, addressing the responsibilities of OMB and federal agencies in the area of information security.[65] The purpose of this subchapter was to:

- Provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources supporting Federal operations and assets;
- Ensuring continued interoperability of Federal Government systems, while implementing proved security management;
- Provide effective Government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security and law enforcement communities;
- Provide for development and maintenance of minimum controls required to protect Federal information and systems; and
- Provide a mechanism for improved oversight of Federal agency information security programs.

---

[62] Intelligence Reform and Terrorism Prevention Act of 2004, Section 102A.(g),"Intelligence Information Sharing," 17 December 2004.

[63] OMB Memo M-00-07, "Incorporating and Funding Security in Information Systems Investments," 28 February 2000.

[64] 44 USC Chapter 35, subchapter II, sections 3531-3536; also Public Law 106-398, Section 1061-1065, "Information Security," 30 October 2001.

[65] House Conference Report 106-945 for NDAA 2001, "Government Information Security Reform," pp. 852–853.

In addition to OMB, GISR laid out specific responsibilities for the Secretary of Defense and the Director of Central Intelligence (DCI), GSA, Departments of Commerce and Justice, and OPM. Federal agencies were directed to appoint a senior information security official who would report to the CIO and be responsible for the execution of the program. Aside from reemphasizing the program responsibilities carried over from CCA 1996, agencies were directed to do an annual evaluation of their information security programs, have an independent audit of their programs, and annually report the findings of both the internal evaluation and the independent audit to OMB. OMB would then compile these reports into a summary report to Congress annually, with the exception of those from DoD and the DCI, who would report separately to the appropriate Congressional committees. GISR contained a sunset provision for two years from the date of enactment (October 2002).

D.1.16 OMB Memo M-01-08[66]

OMB issued this memo to provide guidance on how it expected Federal agencies to carry out the requirements contained within GISR and clarify GISR's relationship to other existing policies regarding information security. The primary focus of this memo, however, was to provide specific details on how the Federal agencies were to comply with the annual reviews, including the reporting requirements and the independent evaluations. It also described how OMB would collect inputs to submit the consolidated report to Congress.

D.1.17 Defense-wide Information Assurance Program (DIAP) 1999[67]

This portion of the U.S. Code mandated an organization created by DoD in 1998 to centralize the oversight for DoD of its information assurance program. It described the responsibilities of the program office, especially its relationship to the DoD CIO, the CCA of 1996, and national critical information infrastructures. The law also directed development of a program strategy and submission of an annual report with specific guidance on the content of that report. When GISR was enacted in 2000, Congress clarified the relationship of the DIAP with the requirements changed in GISR and described the consistency between the annual report of the DIAP and the report required by GISR.[68]

D.1.18 E-Government Act of 2002/Federal Information Security Management Act 2002 (E-Gov Act/FISMA)

Section 3603 of this act mandated the Federal CIO Council, and stated one of its responsibilities was to work with NIST on IT standards, including those for computer security. Title III of this act, the Federal Information Security Management Act of 2002

---

[66] OMB Memo M-01-08, "Guidance on Implementing the Government Information Security Reform Act," 16 January 2001.

[67] 10 USC Sec, 2224, "Defense Information Assurance Program", also Public Law 106-65, Section 1043, 5 October 1999.

[68] Public Law 106-398, Section 1063, "Relationship of DIAP to GISR," 30 October 2000.

(FISMA)[69], provided the primary statutory framework for information assurance in the Federal Government and replaced GISR. It detailed the responsibilities of OMB for this program and delegated certain of these responsibilities to the Secretary of Defense for DoD and DCI for intelligence systems, as well as exempting national security systems from OMB's jurisdiction in certain areas. FISMA required each agency, including agencies with NSS, to develop, document, and implement agency-wide information security programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA continued the annual reporting requirement begun by GISR and mandated the requirement for the operation of the Federal information security incident center (FEDCIRC).

D.1.19 OMB Memos M-03-19[70]/M-04-25[71]

These memos provided detailed guidance to Federal agencies on the reporting requirements to meet FISMA 2002 requirements, incorporating the framework for annual IT security reviews, reporting, and remediation planning contained within the statute. The memos also mandated quarterly updates to OMB on agencies' IT security efforts using quantitative performance measures and their progress in remediation of IT security weaknesses. These measures are then used in the agency's E-Gov scorecard under the President's Management Agenda.[72] The memos highlighted the substantive changes from GISR to FISMA and replaced the OMB Memo M-01-08.

D.1.20 National Strategy for Homeland Security 2002[73]

This strategy lays out the Administration's concept of how it will address the issue of homeland security. As a very high level document, it provided little detail. It states that DHS will place a high priority on protecting the U.S. cyber infrastructure and designates DHS as the lead agency for the Information and Telecommunications sector. It called for DHS to develop and coordinate the implementation of a comprehensive national plan to protect the U.S. infrastructure. DHS was also directed to provide a methodology for identifying and prioritizing critical assets, systems and functions, sharing protection responsibility and establishing standards and benchmarks. Information and Telecommunications was identified in this Strategy as one of the critical infrastructure

---

[69] Federal Information Security Management Act, P.L. 107-347, §§ 301-305, 116 Stat. 2946 (2002). A slightly different version of the same language was enacted as part of the Homeland Security Act of 2002, P.L. 107-296, §§ 1001-1006, 116 Stat. 2259 (2002).

[70] OMB Memo M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting," 6 August 2003.

[71] OMB Memo M-04-25, "FY2004 Reporting Instructions for the Federal Information Security Management Act," 23 August 2004.

[72] The President's Management Agenda, (PMA) announced in the summer of 2001, is an aggressive strategy for improving the management of the Federal government. It focuses on five areas of management weakness across the government where improvements and the most progress can be made. The web site at http://www.whitehouse.gov/results/ provides additional details.

[73] Office of Homeland Security, "National Strategy for Homeland Security," July 2002, pp. 30–33.

sectors.[74] The strategy also states that "while securing cyberspace poses unique challenges and issues…our physical and cyber infrastructures are interconnected" and called for a Strategy to Secure Cyberspace.

D.1.21 National Strategy for Physical Protection of Critical Infrastructures and Key Assets 2003[75]

This document was drafted as a follow-on to the *National Strategy for Homeland Security* partially in response to the call for a comprehensive national plan. It focuses primarily on the physical aspects of critical infrastructures. Although telecommunications is included as a sector in this report, the cyber aspects were only addressed peripherally. The primary focus is on the physical infrastructure of facilities, equipment (such as switches, access tandems and others) connected by fiber and copper cable, and including cellular, microwave and satellite technologies, as well as the wireline network.[76] The purpose of this document was to prioritize and organize procedures to address vulnerabilities, laying out responsibilities of the Federal government, state and local governments and the private sector.

D.1.22 National Strategy to Secure Cyberspace[77]

Called for in the *National Strategy for Homeland Security,* this strategy directed Federal agencies to take specific actions to improve the security of Federal systems. These measures include:

- Continuously assess threats and vulnerabilities to Federal Cyber Systems
- Agency-specific processes:
  - identify and document enterprise architectures
  - continuously assess threats and vulnerabilities
  - implement security controls and remediation efforts.

Additional challenges include:

- authenticate and maintain authorization for users of Federal systems
- secure Federal wireless local area networks
- improved security in government outsourcing and procurement

---

[74] PDD 63 originally called this sector "Information and Communications" and assigned the Department of Commerce as the Sector lead. The National Strategy for Homeland Security retitled the sector "Information and Telecommunications" and changed the sector lead designation to the Department of Homeland Security. It includes what this study calls Cybersecurity, as well as Telecommunications, including the Public-Switched Telecommunications Network (PSTN) and physical infrastructure thereof.

[75] OHS, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," February 2003.

[76] Ibid, "Telecommunications," pp. 47–49.

[77] The White House, "The National Strategy to Secure Cyberspace," February 2003.

- develop specific criteria for independent security reviews and reviewers and certification.

It recommended that DHS use exercises to test the security of Federal systems and to report the results of those exercises to the Director of OMB. It also directed DHS to work with the General Services Administration (GSA) to develop an improved patch management system and to ensure that agencies have made up-to-date security modifications to their software. Finally, it directed DHS to play the central role in implementing the strategy by serving as the primary federal point of contact (POC) for state and local governments, the private sector and the American people on issues related to cyberspace security. Of note, this document called for the review of the NIAP.

D.1.23 Homeland Security Act 2002[78] (HSA 2002)

This act, which created DHS, included the creation of an Assistant Secretary for Infrastructure Protection (ASIP), responsible for the execution of the National Strategies for Physical Protection and to Secure Cyberspace. In the Subsection titled "Information Security", Congress, among other things, authorized the Under Secretary for Information Analysis/Infrastructure Protection (IAIP) to share information and warning on threats and vulnerabilities of critical information systems, coordinate response to threats or attacks on critical information systems, and provide technical assistance with respect to emergency recovery plans responding to major failures of critical information systems with state and local governments, as well as the private sector. It brought together in one organization, entities created as a result of PDD 63: the National Infrastructure Protection Center (NIPC) from FBI; the Critical Infrastructure Assurance Office (CIAO) from Commerce; the National Infrastructure Simulation and Analysis Center (NISAC) from DOE; the Energy Assurance Office, also from DOE; and the Federal Computer Incident Response Center (FEDCIRC) from GSA. The act also created "NetGuard," a program for volunteers with critical skills in information and communications technologies to assist in response these types of emergencies. Finally, the portion of the act titled "Computer Security Enhancement Act" amended sentencing guidelines for certain computer crimes, and commissioned a study and report on the execution of this section.

D.1.24 Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection[79] (HSPD 7)

This document is the most recent administration document establishing national policy for Critical Infrastructure Protection, following the *National Strategy for Homeland Security* and the *National Strategy Physical Protection of Critical Infrastructures and Key Asset.* It officially supersedes PDD 63. HSPD 7 describes the following: (1) the policy concerning protection of the nation's critical infrastructure and key resources; (2) roles and responsibilities of the Secretary of Homeland Security; (3) roles and responsibilities of sector-specific Federal Agencies; (4) roles and responsibilities of other Departments, Agencies and Offices; (5) collaboration with the private sector; and finally,

---

[78] Public Law 107-296, "Homeland Security Act of 2002," Title II-Information Analysis and Infrastructure Protection, sections 201-205, 25 November 2002.

[79] HSPD 7, "Critical Infrastructure Identification, Prioritization, and Protection," 17 December 2003.

(6) implementation details, including the development of an integrated National Plan. This National Plan would include development of sector specific agency (SSA) plans, with the responsibility for Information (Cyber) assigned to the National Cyber Security Division (NCSD) of DHS. Additionally, Federal Department and agency heads were directed, consistent with FISMA, to identify and provide information security protections for their internal critical infrastructure and key resources.

D.1.25 OMB Memo M-04-15[80]

This memo provides implementing direction to Federal departments and agencies on the formal submission of their SSA plans to DHS as directed by HSPD 7. It contains the format to be used by the Federal entities and upon receipt of the plans by DHS, directs an interagency review, to be coordinated by DHS. Included within these plans will be the agency cybersecurity plans that will be reviewed in a manner consistent with reviews of those reports submitted under FISMA. The details of these SSAs include: (1) descriptions of existing capabilities, including personnel and budget; (2) identification of the process for determining budget and personnel requirements for critical infrastructure/key resources (CI/KR) protection, response, and reconstitution activities; and (3) description of the process for ensuring independent oversight of CIP programs. NSCD, as previously mentioned, is responsible for developing the SSA for cybersecurity, which includes its responsibility to coordinate protection, response and reconstitution activities with the Federal agencies and the private sector for cybersecurity. These plans were due to DHS by 31 July 2004. The most recent information indicates that the plans (which were not available for review) will be approved with the National Plan by the Secretary, DHS, in early 2005.

D.1.26 Intelligence Community (IC) Policy

The primary document addressing this area for the IC is the Director of Central Intelligence Directive 6/3 (DCID 6/3).[81] This document established the policy for protection of intelligence information in information systems and assigned responsibility for execution and review of the policy. A companion manual provides the detailed implementation policy as to the expected methods of accomplishing the stated policies.[82]

D.1.27 DoD Policy

DoD policies concerning information assurance (cybersecurity) are discussed in an earlier section. The only current DoD policy concerning cybersecurity as it relates to Critical Infrastructure Protection is DoDD 5160.54. Titled "Critical Asset Assurance Program," it

---

[80] OMB Memo M-04-15, "Development of Homeland Security Presidential Directive (HSPD) 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources," 17 June 2004.

[81] DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems," 5 June 1999.

[82] DCID 6/3 Manual, "Protecting Sensitive Compartmented Information Within Information Systems," downloaded 9 November 2004.

lays out policies and responsibilities for the protection and assurance of DoD critical assets to support DoD missions worldwide.[83]

D.2 Standards/Guidelines

In the computer security environment, the establishment of standards is critical to the ability of an organization to evaluate, acquire and manage applications, products or services. Congress recognized this need and designated Federal government organizational responsibilities for this area.

There are a number of government and private sector entities that develop, promulgate and enforce or promote the use of the standards. Standards, guidelines, best practices, protocols and procedures are defined in Chapter 2 and are used to describe how individuals in an organization should accomplish certain activities. The application of a standard, the most stringent of this group, can be made either mandatory or voluntary by some entity with the authority to do so. An example of a standard is a set of procedures required to be developed by a statute and promulgated and enforced by a Federal department, agency or regulating body that has jurisdiction over that issue. States and local/tribal governments may enact state laws, ordinances, or issue regulations or codes applicable within their jurisdictions that contain or promulgate standards. Compliance normally has some sort of monitoring and enforcement mechanism and penalties to ensure that those entities for which the standard is mandatory do comply. State, local/tribal governments may adopt standards that are made mandatory for the Federal government and make them make them applicable to those organizations under their cognizance. Voluntary standards leave some option to the head of the Federal agency as to whether to adopt in their entirety or in part.

Less stringent than standards are guidelines, which leave the determination of how much if any of their content to be adopted by an organization. There can be a number of guidelines issued that an organization may choose to ignore because they are either not applicable for their circumstance or their circumstance may require similar but different procedures. Best practices are another category of procedures that attempt to describe, for a given set of circumstances, a set of procedures that have proven to be optimal for a given set of conditions. Application of best practices is usually left up to lower level managers who are able to assess the conditions to determine which best practices, if any, are useful. These managers are also the ones who would develop or identify new best practices. Protocols, usually a given set of procedures that should be followed given a certain set of circumstances, are also applicable in cybersecurity and are usually used to describe a set of technical procedures implemented at a software level.

D.2.1 National Institute of Standards and Technology Act 1901, as amended (NIST Act)

NIST's original charter was laid out in what was originally titled the National Bureau of Standards Act (NBSA) of 1901. The National Bureau of Standards was created to …"enhance the competitiveness of American industry while maintaining its traditional function as lead national laboratory for providing the measurements, calibrations, and

[83] DoDD 5160.54, "Critical Asset Assurance Program (CAAP)," 20 January 1998.

quality assurance techniques which underpin United States commerce, technological progress, improved product reliability and manufacturing processes, and public safety; (2) to assist private sector initiatives to capitalize on advanced technology; (3) to advance, through operative efforts among industries, universities, and government laboratories, promising research and development projects, which can be optimized by the private sector for commercial and industrial applications; and (4) to promote shared risks, accelerated development, and pooling of skills which will be necessary to strengthen America's manufacturing industries…." [84] These functions formed the foundation on which the National Institute for Science and Technology became a critical institution in the development and promulgation of cybersecurity standards and procedures as directed in other, more recent statutes.[85]

D.2.2 CSA 1987

This statute amended the NIST Act by establishing a computer standards program and assigned NIST the responsibility to develop standards and guidelines for Federal computer systems on the security and privacy of sensitive information. Specifically NIST was responsible for:

- Developing standards, guidelines and associated methods and techniques for computer systems;
- Except for NSS, develop uniform standards and guidelines for Federal computer systems;
- Develop technical, management, physical and administrative standards and guidelines for security and privacy of sensitive information in Federal computer systems;
- Submit standards and guidelines, along with recommendations as to which should be made compulsory and binding, to the Secretary of Commerce for promulgation to Federal agencies;
- Develop guidelines training for operators in security awareness and accepted security practice;
- Develop validation procedures for, and evaluate the effectiveness of standards and guidelines promulgated under the CSA through research and liaison with other government and private agencies;
- NIST was also supposed to draw on the work done by NSA for the national security community where such work is consistent with its other efforts for protecting sensitive information in Federal computer systems.

The Secretary of Commerce was authorized to promulgate standards and guidelines pertaining to Federal computer systems and to make such standards compulsory and binding to the extent deemed necessary. Only the President could disapprove or modify

---

[84] 15 USC Chapter 7, section 271, National Institute of Standards and Technology, August 23, 1988.

[85] 15 USC section 278g-3, "NIST," Computer Standards Program, 25 November 2002.

these standards. The statute provided a process, however, by which these computer security standards could be waived by the Secretary of Commerce if it was determined that compliance would adversely affect the accomplishment of the mission or cause a major financial impact not offset by Government-wide savings. The Secretary could delegate to the head of Federal agencies the authority to waive such standards and who could then further delegate this authority to certain senior officials of the agency.

D.2.3 National Technology Transfer and Advancement Act of 1995 (NTTAA 1995)[86]

The significance of this Act for cybersecurity for the Federal Government is that it did two things: (1) assigned NIST the responsibility for comparing standards used in a variety of venues with the standards adopted or recognized by the Federal Government and coordinating the use of private sector standards by Federal agencies;[87] and (2) required all Federal agencies and departments to use technical standards developed or adopted by voluntary consensus standards bodies, except where inconsistent with applicable law or otherwise impractical.[88] Federal agencies are encouraged to participate in these standards bodies to the extent practicable to ensure that their concerns are addressed in the development of the voluntary consensus standard by the standards body. The significance of this Act is that, where no Federal or agency standard exists for Federal agencies to implement and a voluntary consensus standard exists, the adoption of this voluntary consensus standard becomes mandatory by Federal agencies.

D.2.4 OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Activities, 10 Feb 1998

This Circular provides implementing direction to Federal Agencies for the NTTAA of 1995. It clarifies the applicability of this policy and defines some of the terms found in the Act. "Voluntary consensus standards are defined as "those standards developed or adopted by voluntary consensus standards bodies, both domestic and international."[89] The Circular restates the policy requirement for Federal agency adoption of voluntary consensus standards and established a annual reporting requirement for Federal agencies on decisions to use government-unique standards in lieu of voluntary consensus standards.[90] Although not specific to cybersecurity, this Circular has implications for the Standards development and implementation for Federal agencies.

---

[86] Public Law 104-113, "National Technology Transfer and Advancement Act of 1995," 7 March 1996.

[87] Ibid, Section 12, para (a)(3).

[88] Ibid, Section 12, para (d) (1) and (d)(3).

[89] OMB Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities", 10 February 1998, para 4.a.

[90] Ibid, para 9.

D.2.5 15 CFR Part 287, Guidance on Federal Conformity Assessment Activities, 10 August 2000[91]

This document provides policy guidance to Federal agencies on the evaluation of conformity assessment activities relative to NTTAA 1995. "Conformity assessment" is defined as any activity concerned with determining directly or indirectly that requirements are fulfilled or requirements for products, services, systems, and organizations defined by law or regulation or by an agency in a procurement activity and includes accreditation, certification and inspection.[92]

D.2.6 CCA 1996

This act made some significant changes in the Standards area, beginning with giving the Director of OMB oversight responsibility for the development and implementation of standards and guidelines developed by the Secretary of Commerce, through NIST, as required by the CSA of 1987.[93] As this act repealed the section of the CSA concerning the authority of the Secretary of Commerce to make certain standards and guidelines compulsory and binding for Federal agencies, CCA clarified that authority, including the ability to waive standards. It was specified that the authority to waive standards could only be delegated as far as the CIOs of organizations identified within the act. EO 13011 was issued by the Administration in 1996 as described in an earlier section, and established a Government Information Technology Services Board. This Board, among other things, was responsible for making recommendations and assisting with developing, with NIST and established standards bodies, standards and guidelines pertaining to Federal information systems.[94] The responsibilities of the Secretary of Commerce were reiterated, with the additional duty of taking into consideration the recommendations of the agencies, the CIO Council, and the aforementioned Services Board.[95]

D.2.7 OMB Circular A-130

This circular reiterated the responsibilities of both Federal agencies, in general, and the Department of Commerce, in specific, regarding the use and development of standards. OMB directed Federal agencies to use voluntary standards and Federal Information Processing Standards (FIPS) (promulgated by NIST) where appropriate or required. Agencies were required to implement policies, standards and procedures issued by OMB, the Department of Commerce, GSA and OPM. Agencies were also responsible for incorporating the more stringent standards for national security systems as appropriate. OMB directed the Secretary of Commerce to develop and issue FIPS and guidelines to ensure efficient and effective security of information technology, taking into consideration recommendations of agencies and the Federal CIO Council.

---

[91] 15 CFR Part 287, "Guidance on Federal Conformity Assessment Activities," 10 August 2000.

[92] Ibid, Section 287.2.

[93] ITMRA Title III, Subtitle A, Section 5112 (d).

[94] EO 13011 Sec. 4 (a)(4).

[95] EO 13011 Sec 8.

D.2.8 FISMA 2002

This statute made substantial changes in the standards area for IT and IT security. In general, heads of Federal agencies were required to comply with information security standards promulgated under this act and information system security standards for national security systems. The Secretary of Commerce was given the authority to make mandatory the standards and guidelines developed by NIST and, further, were required to act on any standards/guidelines submitted by NIST within 6 months of receipt. These mandatory standards and guidelines could only be modified or disapproved by the President. Heads of Federal agencies were allowed apply more stringent standards and guidelines, but must include these mandatory standards and guidelines.[96]

The Director of OMB was responsible for providing oversight of the development of standards and guidelines for information security and ensuring that these standards are coordinated with those entities responsible for developing standards and guidelines for national security systems to ensure they are complementary.[97]

FISMA also provided significant direction to NIST directly, on the standards to be developed, including a definition of what constituted minimum security standards. NIST was directed to work with NSA to ensure that standards developed for Federal agencies were consistent with those developed for NSS. Additionally, NIST was directed to submit those standards that should be made mandatory to the Secretary of Commerce within 12 months, taking into consideration any recommendations from the Information and Security Privacy Board.[98] This Board, formerly called the Computer System Security and Privacy Advisory Board, was given the charter to advise the Secretary of Commerce, and Director, OMB, on a number of information security matters, including reviewing and recommending proposed standards and guidelines.[99] This statute also repealed the section of the CSA, which had authorized the Secretary of Commerce to waive standards that were made compulsory and binding, with the ability to further delegate that waiver authority to senior officials of Federal agencies.[100]

D.2.9 OMB Memo M-03-19[101]

In this memo, OMB outlines the changes in policy brought about by FISMA and provides additional policy direction to Federal agencies as a result of that statute. The memo reiterates the direction to NIST concerning compulsory and binding standards and encourages agencies to participate in the drafting and review of these drafts. OMB will issue, as needed, accompanying implementing guidance for the NIST standards and guidelines.

---

96 Section 11331, title 40 US Code, "Responsibilities for Federal Information Systems Standards."

97 Sec 301, subsection 3543.

98 Section 303 FISMA, which amended section 20 of the NIST Act (15 USC 278g-3).

99 Section 302 FISMA, which amended section 21 of the NIST Act (15 USC 278g-4).

100 Section 303 FISMA, which amended section 20 of the NIST Act (15 USC 278g-3).

101 OMB Memo M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting," OMB, Washington, D.C., 6 August 2003.

D.2.10 NIST Standards and Guidelines

The mandatory Federal Information Processing Standards (FIPS) issued by NIST primarily deal with various encryption schemes, although that situation is changing as NIST finalizes the coordination of more FIPS to meet the minimum set required by FISMA 2002. The more widely applicable guidance for security procedures and incident handling are addressed in Special Publications (SP) that are voluntary and may be selectively, implemented, if at all. OMB has made only one SP mandatory, but strongly encourages Federal agency heads to comply to the maximum extent possible, with other applicable SP.

As a result of the tasking to NIST regarding standards and guidelines, NIST has issued a number of FIPS (Federal Information Processing Standards) and SP (Special Pubs) addressing aspects of information security. Some of these documents are mandatory, while others are voluntary. A list of these documents is provided at Table 1 in Chapter 3. Copies of the majority of the documents are available at the following url: http://csrc.nist.gov/publications/index.html.

D.2.11 National Security Standards and Guidelines

National security systems are exempt from the standards and guidelines promulgated by NIST for the Federal government. Standards and guidelines for national security systems are developed, prescribed, enforced and overseen as authorized by law and as directed by the President.[102] As the Executive Agent for NSS, SECDEF approved and provides minimum security standards and doctrine for NSS. DIRNSA, as the National Manager for NSS, is responsible for reviewing and approving all standards, techniques, systems and equipment related to the security of national security systems and coordinating with NIST as required by the CSA of 1987 (as modified by FISMA). FISMA requires Federal agencies with national security systems to comply with standards and guidelines developed for NSS as described above. CNSS has issued detailed policy and guidance to the national security community under its authority per NSD 42.[103]

D.2.12 Department of Defense Standards and Guidelines

The authority to develop standards for DoD was delegated to Assistant Secretary of Defense for Network Infrastructure Interoperability (ASD(NII))/DoD CIO for information assurance standards, in cooperation with NSA, and to the Defense Information Systems Agency (DISA) for IT standards. DoD has long recognized the need for standards and guidelines to manage its IT infrastructure, and in particular, information security/assurance. The primary policy document for the IT infrastructure is DoDD 8100.1 Global Information Grid Overarching Policy[104] that implements the requirements of the Clinger-Cohen Act for DoD. The document addressing standards and guidelines

---

[102] 40 USC ss11331, para (a)(2)).

[103] The complete list of those documents is found in the Index of National Security Systems Issuances, dated October 2004 and is maintained by the CNSS Secretariat, located at NSA. This index can be found at the following url: http://www.nstissc.gov/html/library.html.

[104] DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," 19 September 2002.

for information security/assurance is DoDD 8500.1[105] and its companion Instruction DoDI 8500.2,[106] already mentioned in the cybersecurity theme. Heads of DoD components are responsible and accountable for implementing these standards within the parts of the DoD IT infrastructure under their operation and control and may incorporate more stringent standards, as long as interoperability across the DoD IT infrastructure is not impacted.

D.2.13 Intelligence Community Standards and Guidelines

As directed in the National Security Act of 1947[107] and reinforced by EOs12333,[108] and 13355,[109] the DCI has oversight of the Intelligence Community and authority to develop policies, procedures and standards for activities of the Federal agencies that fall within the IC. This is separate and above the DCI's responsibilities for the CIA, similar to SECDEF's executive agent responsibility for NSS. The most recent document, IRTPA 2005, designated the Director of National Intelligence (DNI) as the head of the intelligence community with the authority to "…establish uniform security standards and procedures; and establish common information technology standards protocols, and interfaces…."[110]

Two primary documents addressing IC concerns with regard to protecting sensitive compartmented information (SCI) within information systems: DCI Directive 6/3 Policy and its accompanying Manual.[111] As mentioned previously, it is in these documents that the DCI lays out the standards and guidelines regarding information security in those systems of interest. Federal agencies having components designated as part of the IC must implement these requirements.

D.2.13.1 National Security Act of 1947 (NSA 1947)

Gives the DCI authority to develop policies, procedures and standards for activities of the Federal agencies that fall within the Intelligence Community.

---

[105] DoD Directive 8500.1, "Information Assurance," 24 October 2002.

[106] DoD Instruction 8500.2, "Information Assurance (IA) Implementation," 6 February 2003.

[107] National Security Act of 1947, as amended, 26 July 1947, "Responsibilities of the Director of Central Intelligence," Sections 103-104.

[108] EO 12333, "United States Intelligence Activities," para 1.5 "Director of Central Intelligence," 4 December 1981.

[109] EO 13355, "Strengthened Management of the Intelligence Community," Section 2, (b), 27 August 2004.

[110] Intelligence Reform and Terrorism Prevention Act of 2004, Section 102A.(g),"Intelligence Information Sharing," 17 December 2004.

[111] Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," 5 June 1999.

D.2.13.2 Intelligence Reform Act of 2004 (IRA 2004)

Gives the Director of National Intelligence (DNI), as head of the intelligence community, authority to "…establish uniform security standards and procedures; and establish common information technology standards protocols, and interfaces…."[112]

Collectively, these statutes established the requirement for standards and guidelines for the Federal government and assigned the responsibility for developing and promulgating these standards and guidelines either to NIST, the Secretary of Defense, or the head of the Intelligence Community.

D.2.14 National and International Standards Bodies

The discussion of standards would be incomplete if it did not include the existence of national and international standards bodies, outside of the Federal government. These bodies issue standards that have been developed by technical committees representing the private sector, academia and government activities. NIST, DoD, NSA and a number of Federal government organizations participate on a regular basis in developing these standards, particularly those having a specific application in their area of interest or responsibility. These standards are voluntary unless adopted by an oversight organization with the authority to enforce implementation. Examples include: American National Standards Institute (ANSI), Institute for Electrical and Electronics Engineers (IEEE), International Telecommunications Union (ITU), Internet Engineering Task Force (IETF) and others. An example of a standard developed by one of these bodies is ISO/IEC 17799 that provides an international agree-upon standard for information security management.[113]

D.2.15 Best Practices

The most flexible category of the standards/guidelines area is that of "best practices." "Best practices" refers to strategies, policies, procedures and other action-related elements of cybersecurity that are generally accepted as being the most successful or cost-effective. Many organizations sponsor or encourage the development of best practices, partially in an effort to get input from disparate organizations within government and in the private sector, but also to build consensus on general practices without resorting to issuance of policies and regulations.[114] NIST's Computer Security Division (CSD) hosts the Federal Agency Security Practices (FASP) for the Federal CIO Council that provides a mechanism for information sharing and collaboration for Federal security professionals. It also contains links to a number of public and private sector best

---

[112] Intelligence Reform Act of 2004, Section 102A.(g),"Intelligence Information Sharing," 17 December 2004.

[113] ISO/IEC 17799, "Information Technology: Code of Practice for Information Security Management," First Edition 2000-12-01.

[114] The FCC's Network Reliability & Interoperability Council is one example of a regulatory advisory group sponsoring best practices in telecommunications/Cybersecurity to prevent having to issue controversial and expensive regulations. Web address is: http://www.bell-labs.com/cgi-user/krauscher/bestp.pl.

practices sites for additional information.[115] "Best Practices" can provide useful information to assist these professionals, but the voluntary nature and varying technical detail can prove problematic in implementation and consistency.[116]

D.2.16 Applicability of Requirements

One of the difficulties in policy implementation is that Federal agencies are required to identify the community of interest in which each IT system belongs. Table 20 illustrates how Federal agencies IT systems may be identified with multiple communities and be subject to various requirements. It is possible that a single Department may have entities and systems belonging to all four communities of interest and must, therefore, implement four sets of policies. The DoD, for example, has systems that fall in four communities of interest. To simplify the issue, Departments or Agencies have the authority to adopt more stringent policies and can thereby reduce the implementation complexity by bringing all of their systems under one or two sets of policies. A case in point, once again, is the DoD. NSTISSP 11 requires all computer security products introduced into National Security Systems be certified through the NIAP process. National Security Systems explicitly exclude systems used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). As a result, if a Department or Agency adopts these requirements throughout its respective organization, some systems owned or operated by or on behalf of these organizations may nonetheless not be covered by this requirement. In DoD's case, DoDD 8500.1 [DoD2002a] requires ***all*** DoD systems meet NSTISSP 11 requirements, eliminating different standards for National Security Systems and the rest of the systems in DoD. For Federal agencies that do not adopt a single set of standards, the challenge becomes which set of standards applies to which IT systems in a consistent, coherent way, at the same time ensuring that the application of these standards does not result in non-interoperable systems.

---

[115] Web site address is: http://csrc.nist.gov/fasp/.

[116] A good discussion of the limitations of the use of best practices is contained in the following report: Fischer, Eric A, "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options," RL3277, 22 February 2002, p. 38.

Table 20. Federal Departments and Agencies and Communities

Federal Departments and Agencies			Intelligence Community	National Security Community	Federal Government
CIA					
	DDCI/CM				
Defense					
	Air Force				
		AF Intel.			
	Army				
		Army Intel.			
	Navy				
		Navy Intel.			
	Marine Corp				
		MC Intel.			
	DIA				
	JCS				
	NGA				
	NRO				
	NSA				
	DISA				
	DTRA				
	DLA				
State					
Treasury					
Energy					
Justice					
	FBI				
Homeland Security					
	Coast Guard				
		CG Intel.			
	FEMA				
	NCS				
Commerce					
	CIAO				
Health and Human Services					
Transportation					
GSA					
OSTP					
Agriculture					
Education					
Housing and Urban Development					
Interior					
Labor					
Veterans Affairs					

D.3 Education, Training, and Awareness

Education, training and awareness (ET&A) are critical components of any information security program. Requirements for these activities are contained in numerous policy documents, along with specific assignments of responsibility.

D.3.1 CSA 1987/NIST Act

The CSA, for the first time, required mandatory periodic computer security training of all Federal personnel involved in the management, use or operation of Federal computer systems containing sensitive information.[117] As modified by CSA, NIST was given two tasks that focus on training: (1) develop guidelines for use by Federal personnel in training their employees in security awareness and accepted security practice; and (2) assisting the Office of Personnel Management (OPM) in developing regulations pertaining to training in this area. Further detail is provided in the Act on the objectives of this training. Additionally, OPM was directed to issue regulations concerning the scope and manner of this training.[118]

D.3.2 CCA 1996

This statute contained additional tasking regarding education and training. First, it assigned the responsibility for monitoring the status of training of Federal personnel to the Director, OMB. Additionally, Chief Information Officers (CIO) of Federal agencies, were responsible for training their IT personnel. The training cited was not specific to information security, but concerned information technology generally as follows:

> "…The Director [OMB] shall monitor the development and implementation of training in information resources management in executive agency personnel…."[119]

CIO's of agencies shall "…in order to rectify any deficiency in meeting those requirements, develop strategies and specific plans for hiring, training, and professional development…."[120]

It is clear that the statute intended for the CIOs of Federal agencies to ensure that they had sufficient numbers of trained personnel to carry out the information technology requirements, including that of information security.

D.3.3 EO 13011 Federal Information Technology

This EO was the initial Executive Branch document to implement the requirements of the CCA. It laid out the responsibilities of Agency Heads and included support for appropriate training of personnel in this area. It also established the Chief Information Officer Council (Federal CIO Council) and assigned that body the responsibility for assessing and addressing the hiring, training, classification, and professional development needs for IT management.[121]

---

[117] CSA, Section 2.(b)(4).

[118] Ibid, Section 5, "Federal Computer System Training."

[119] CCA, Pub Law 104-106, Section 5112, para (i).

[120] Ibid, Section 5125, para (c)(3)(C).

[121] EO 13011, "Federal Information Technology," 16 July 1996, Sections 2 and 3.

D.3.4 OMB Circular A-130

This document repeated the training requirements stated in CCA. OPM was specifically charged with developing and conducting training programs for Federal personnel on information resources management; evaluating future personnel management and staffing in this area, and developing training programs for Federal personnel in the design, operation or maintenance of information systems.[122] The Circular Appendix on Security provides additional details on the required training. Specifically, agencies are required to implement and maintain automated information security programs that, among other things, ensure that all individuals are trained in how to fulfill their security responsibilities before allowing them access to the system, demonstrate appropriate behavior while on the systems; and receive periodic refresher training for continued access to systems.[123] Specialized training for personnel is required for major applications.[124] OPM has two additional responsibilities in information security training (1) ensuring that its regulations concerning computer security training are effective; and (2) assisting the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.[125]

D.3.5 FISMA

This statute took security training requirements laid out in the CSA and expanded them. Agencies CIOs were tasked with ensuring that IT personnel with significant security responsibilities were trained.[126] The CIOs must also ensure they have sufficient numbers of trained personnel to handle their designated responsibilities.[127] Additionally, agencies, as part of their information security program, must conduct security awareness training for all personnel, including contractors, of both the information security risks associated with their responsibilities and their responsibility to comply with agency policies and procedures intended to reduce these risks.[128] Finally, this training must be documented in the performance plan that agency CIOs submit to OMB.[129]

---

[122] OMB Circular A-130, Section 9.f.

[123] Ibid, Appendix III, "Security of Federal Automated Information Resources," para A.3.a.20, b.

[124] Ibid, para A.3.b.2.b.

[125] Ibid, para A.4.e.

[126] FISMA, 44 USC 35, section 3544, para (a)(3)(D). However, clarification of what Congress or OMB meant by significant is not defined, leaving some confusion as to the distinction between significant and non-significant for the purposes of this requirement.

[127] Ibid, para (a)(4).

[128] Ibid, para (b)(4).

[129] Ibid, para (d)(1)(B).

D.3.6 OMB Memo M-03-19

This memo provided additional guidance to the Federal agencies on reporting requirements for FISMA. That guidance also included a requirement to report on the status of security training and awareness of agency employees (including contractors). [130]

D.3.7 OPM Personnel Regulations for Federal Personnel

OPM issued its regulation prescribing mandatory information security training for Federal personnel, originally in 1991, and revised it in 2004 to bring the regulation into compliance with FISMA.[131] The regulation directs Executive Agencies to develop information systems security awareness training plans, including specific training targeted at individuals identified as having significant information security responsibilities. All users are required to have initial training prior to being allowed access to systems, annual awareness training, and additional training when there is a significant change in responsibilities. Standards and guidelines for training are provided through NIST and are described in the next paragraph.

D.3.8 NIST Standards and Guidelines for Training for Federal Personnel

As directed by CSA, NIST developed standards and guidelines for information security training for Federal agencies. It is contained in two documents, NIST SP 800-16 and 800-50.[132] The learning continuum modeled in this guidance provides the relationship between awareness, training, and education. The first document contains a methodology that can be used to develop training courses for a number of audiences, which may have significant information security responsibilities. The second document is intended to aid Federal agencies in developing and information security FISMA compliant ET&A program. Additionally, through their Computer Security Resource Center web site, NIST provides a mechanism to promulgate timely information to the information security community. The web site address for the ET&A information can be found at http://csrc.nist.gov/ATE.

D.3.9 National Security Systems Education and Training Requirements

As the National Manager for NSS, NSA is responsible for development of standards for education and training for the national security community. It has issued two policy directives and four instructions (during the period 19xx-200x) containing national training standards for individuals with responsibilities in information security. These documents reflect NSA's understanding that individuals with differing responsibilities in information security need different levels and types of training. They provide a detailed roadmap for Federal agencies with national security systems to incorporate into their own programs. The specific documents are:

---

[130] OMB Memo M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting," 6 August 2003.

[131] 5 CFR Part 930, subpart C, "Information Security Responsibilities for Employees who Manage or Use Federal Information Systems," 14 June 2004.

[132] NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998 and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

D.3.9.1 NSTISSD No. 500, "Information Systems Security (INFOSEC) Education, Training and Awareness," 25 February 1993.

D.3.9.2 NSTISSD No. 501, "National Training Program for Information Systems Security (INFOSEC) Professionals," 16 November 1992.

D.3.9.3 NSTISSI No. 4011, "National Training Standards for Information Systems Security (INFOSEC) Professionals," 20 June 1994.

D.3.9.4 CNSSI No. 4012, "National Information Assurance Training Standards for Senior System Managers," June 2004.

D.3.9.5 CNSSI No. 4013, "National Information Assurance Training Standard for Systems Administrators," March 2004.

D.3.9.6 CNSSI No. 4014, "National Assurance Training Standard for Information Systems Security Officers," April 2004.

D.3.9.7 NSTISSI No. 4015, "National Training Standards for System Certifiers," December 2000.

D.3.10 DoD Education and Training Requirements

DoD has a detailed education, training and awareness programs for its personnel for a variety of areas and a rigorous program of how to do education, training, and awareness (ET&A), particularly for its uniformed personnel since their ET&A is tied to career fields at both the enlisted and officer level. There are three primary documents addressing information security/awareness training: (1) DoDD 8500.1, which contains the primary direction for IA training for all and for specific responsibilities for IA,[133] (2) DoDI 8500.2, which provides some additional details on who should be trained in IA[134]; and (3) DODD 8570.1, which provides extensive detail on ET&A for the IA workforce, including certification requirements for individuals with certain designated responsibilities for IA,[135] There is a companion manual for the last document, which provides guidance and procedures for the IA workforce ET&A in draft that is awaiting final approval.

D.3.11 Intelligence Community Education and Training Requirements

In DCID 6/3, the DCI is required to establish and maintain a formal information security education, awareness and training program. Also included were the agencies, departments and components of the IC. Specifically, since this document primarily addresses the Certification and Accreditation process (C&A) for allowing systems to operate and connect in the IC, the education, training and awareness requirements are geared towards individuals who are involved in this process. DCID 6/3 spells out the details of the education, training and awareness requirements and included that for

---

[133] DoDD 8500.1, "Information Assurance," 24 October 2002, para 4.22.

[134] DODI 8500.2, "Information Assurance Implementation," 6 February 2003, para 5.7.7.

[135] DODD 8570.1, "Information Assurance Training, Certification, and Workforce Management," 15 August 2004.

individuals with specific responsibilities for the C&A process, as well as what general users' training should address.[136]

D.4 Research

This section examines the statutory and policy requirements for the NIAP research. The review of relevant statutes and policies for the NIAP research guidance encompassed all of the documents discussed in the body of this report, but only those documents specifically mentioning research are discussed here. The foundation for this portion of the report is the relevant portion of the NIAP memorandum of agreement and the stated and implicit agreement within it to undertake the research required to achieve the NIAP's stated objectives. Specifically, in the memorandum, the two parties agree to employ the latest techniques to develop specification-based tests, methods, and tools to provide objective measures for evaluating quality and security. They also commit to collaborative research to develop the test methods. The research required to develop objective measures has been lacking. However, this is not the only NIAP-related research shortfall.

Because of the volatility of the cybersecurity arena, due to new attacks being invented each day as well as the deployment of new information technologies, there is a significant need for research to develop the tools and techniques needed to continue to effectively execute NIAP-related activities. However, to date, very little of the necessary NIAP-specific research infrastructure has been assembled and, as a result, the NIAP functions by exploiting research developments achieved for other purposes. Because the NIAP is forced to re-purpose research results, there are technological aspects of the NIAP process that remain uninvestigated even though these technology aspects are important to the NIAP process.

To clearly present the statutory and policy guidance as it relates to the NIAP, each portion will be examined in turn. The following table (Table 21) presents the statutory and policy provisions regarding research that are NIAP related.

[136] DCID 6/3, "Protecting Sensitive Compartmented Information within Information Systems," Policy, 5 June 1999, para B.3.c.; Manual, para 8.b.1.

Table 21. Legislation Regarding NIAP-Related Research

	DoD	NIAP-related NIST	NSF	NIST	Other Federal
Research on vulnerability assessments and techniques for quantifying risk		CCA 1996			
Cyber security research, development of research centers, research grants, fellowships, education	NDAA 2001		CSR&DA 2002	CCA 1996 HSA 2002	CSA 1987
Determine nature and extent of computer vulnerabilities, develop cost-effective computer security techniques,				HSA 2002 FISMA 2002 3) E-Gov 2002	
Review private sector information security policies, assess standards and guidelines, and apply select critical infrastructure protection technologies to other systems				HSA 2002	
Assess utility of tamper-resistant security software and other security tools to protect critical C3I	NDAA 2004				
DARPA and NSA coordinate research efforts for information assurance research	DoDD 8500.1				

D.4.1 Relevant Statutory Provisions

Regarding the need for further research within the statutory arena, overall there appears to be an implicit assumption that there will be adequate research conducted to support attainment of the NIAP goals. While some statutes contain mandates for research, most are by and large silent on the subject of NIAP-relevant research.

D.4.2 Computer Security Act 1987 (CSA 1987)

This statute calls for a research program in computer security and for research to protect computer assets from attack. None of the research called for in the act is directly targeted at supporting the NIAP, but some results, such as metrics development, that would derive from the research that is suggested could serve to improve the NIAP process.

D.4.3 Clinger-Cohen Act 1996 (CCA 1996)

CCA 1996 authorizes expenditures for cybersecurity research to enhance computer security. Within the act, there are a number of research mandates imposed, most of which are to be addressed by the National Science Foundation. However, within the list of research areas called out by the act, there is only one that is applicable to the NIAP. That provision calls for research on vulnerability assessments and techniques for quantifying risk. The research is to be performed under the aegis of the National Science Foundation (NSF); however, since NSF's mandate is to pursue fundamental/foundational research, aligning their computer security research goals to meet even this need of the NIAP would

be challenging at best. Within the act, other appropriations are authorized for development of research centers, grants, and education for cybersecurity, none of which are specifically targeted at the NIAP needs.

D.4.4 Homeland Security Act 2002 (HSA 2002)

This statute tasks the National Institute of Science and Technology to perform research related to computer security, to determine the nature and extent of information security vulnerabilities, and to develop techniques for providing cost-effective information security. The act also tasks NIST to review policies for private sector information security, to determine those techniques developed to protect national security systems that can be used to protect other systems to increase their information security, and to assess standards and guidelines. Here again, the research tasking does not directly address the NIAP needs and the NIAP is not specifically addressed in the act.

D.4.5 E-Government Act 2002 (E-Gov 2002)

This Act tasks NIST with the responsibility to conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security. However, the act also tasks NIST with the responsibility for developing and periodically revising performance indicators and measures for agency information security policies and practices; a tasking that does support the NIAP needs to some degree.

D.4.6 Federal Information Security Management Act 2002 (FISMA 2002)

FISMA 2002 requires NIST to conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.

D.4.7 Cyber Security Research and Development Act 2002 (CSR&DA 2002)

This statute provides $903 million over 5 years for cybersecurity research and education programs. This statute directs the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. The statute also directs NIST to create new program grants for partnerships between academia and industry.

D.4.8 NDAA 2001

DoD was required by this Act to establish an Institute for Defense Computer Security and Information Protection. The Institute would conduct research relevant to foreseeable computer and network security requirements and information assurance requirements of the Department of Defense. The principal foci of the Institute would be on addressing research areas not being addressed by other organizations in the private or public sector and facilitating the exchange of information regarding cyberthreats, technology, tools, and other relevant issues. Grant, education, and centers of excellence programs were also established and funded.

D.4.9 NDAA 2004

This Act contains no direct provisions for NIAP research, but it does direct the Secretary of Defense to assess the utility of tamper-resistant security software and other innovative software security tools in protecting critical DoD command, control, communications and

intelligence software and to incorporate such protections where they are effective, which by implication requires a study/survey of technologies. The results of this study/survey would be applicable to the NIAP.

D.4.10 The Health Insurance Portability And Accountability Act Of 1996

This Act contains no provisions for information security research or information assurance research. We mention this act, even though it contains no research provisions, to highlight the fact that this act imposes implicit demands for major advances in cybersecurity but does not discuss these advances, provide a framework for them, or mandate them. The **Gramm-Leach-Bliley Act** also contains no provisions for information security research or information assurance research, but is mentioned for the same reason as the Health Insurance Portability and Accountability Act Of 1996.

D.4.11 Relevant Policy Provisions

D.4.11.1 National Strategy to Secure Cyberspace

This document states that the Federal government should support research and technology development to enable the private sector to better secure privately-owned portions of the national critical infrastructure. The document also points out that DHS is responsible for performing and funding research and development leading to new scientific understanding and technologies to support homeland security, and by implication cyberspace. The document also recommends that the Federal Government prioritize cybersecurity research and development agendas, as one of eight major actions to be undertaken. It is pointed out that "An important goal of cybersecurity research will be the development of highly secure, trustworthy, and resilient computing systems," but specifics concerning prioritization or process to achieve this objective are not discussed. The emergence of new technologies in cyberspace, such as optical computing and nanotechnology, are raised as factors influencing cybersecurity in the future. Several research priorities are identified, but neither the NIAP nor any of its supporting technologies are among them.

D.4.11.2 HSPD 7

This directive does establish some research policy guidance. It requires the Department of Commerce to work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts. This activity includes using Commerce's authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

D.4.11.3 DODD 8500.1

This requires the director of DARPA to coordinate research efforts in the information assurance arena with the director of NSA.

D.4.12 Research Implementation Issues

The documents referenced in the next section discuss implementation issues for Research.

D.4.12.1 Status of the Federal Critical Infrastructure Protection Activities

This 2001 report to the President examines the needs and accomplishments of the different departments and agencies of the Federal Government as regards Critical Infrastructure Protection as of the date of the report. The report points out the need for research across a broad front that addresses a wide variety of cybersecurity research topics. The topics that are identified are department and agency specific as well as overarching research needs, some of which may be re-purposed for use within the NIAP.

D.4.12.2 Information Security and Privacy Advisory Board

An ISPAB **report** in 2004 takes note of the need for additional funding in the area of cybersecurity and for developing standards and guidelines that serve to protect the cyber infrastructure. The Board is critical of progress to date and that "Legislation enacted by Congress in recent years (e.g., FISMA and the Cyber Security R&D Act) suggests that the Congress recognizes that need but the programs authorized in those Acts have not been funded." Additionally, they note that "While funding for the program in real terms has grown modestly, it has not kept pace with the growing demand for cybersecurity guidelines and standards as a result of the Government and the nation's growing reliance of information technology, the growth and diversity of the technologies on which we have come to depend, and the increased threat." They conclude that current levels of funding are inadequate.[137]

D.4.12.3 General Accountability Office (GAO) reports

D.4.12.3.1 GAO 2003 High-Risk Series report: Protecting Information Systems: Supporting the Federal Government and the Nation's Critical Infrastructures

This report notes the need for continued research in the field of information assurance. The report notes that there is an ongoing need for research and that funding for information assurance research has been authorized over a five-year period from 2003–2008 but delves no deeper into the research issues associated with information security or the NIAP.

D.4.12.3.2 GAO report GAO-04-321 - Cybersecurity for Critical Infrastructure Protection

In this report, GAO found that "Despite the availability of current cybersecurity technologies, there is a demonstrated need for new technologies. Long-term efforts are needed, such as the development of standards, research into cybersecurity vulnerabilities and technological solutions, and the transition of research results into commercially available products." In the report, the GAO also notes that "several standards exist for cybersecurity technology in the areas of protocol security, product-level security, and operational guidelines; there is still a need to develop standards that could help guide the use of cybersecurity technologies and processes." Furthermore, the report states that

---

[137] ISPAB, "NIST Computer Security Division: The Case for Adequate Funding," June 2004. Document available at http://csrc.nist.gov/ispab/bd-recommendations/ISPAB-ReportAdequateFundingNIST-CSD.pdf.

there is a need for research to address future security needs, "possible long-term research areas include tools for ensuring privacy, embedding fault-tolerance in systems, self-managing and self-healing systems, and re-architecting the Internet" as well as research into security issues related to control of critical infrastructure. The report reprises the discussion here of several of the major statutes affecting information security, and uses these statutes as a jumping-off point to call for additional research into security technologies affected by the statutes. The report identifies several technological areas in need of further research efforts; these areas include (1) composing secure systems from insecure components, (2) security for network embedded systems, (3) security metrics and evaluation, (4) the socioeconomic impact of security, (5) vulnerability identification and analysis, and (6) wireless security. Note that, while not specifically mentioned, the need for further work on metrics and evaluation is relevant to the NIAP and indicates that it is believed that we lack adequate means for assessing the security properties of an application.

D.4.12.4 Department of Defense Reports

D.4.12.4.1 1996 Report of the Defense Science Board on Information Warfare Defense[138]

This report states that there is a need for an ambitious research program for information warfare defense. However, even though they do not specifically address the needs of the NIAP directly, they do call for a vigorous research program in all areas of information warfare defense.

D.4.12.4.2 2001 Report of the Defense Science Board on Defensive Information Operations[139]

This report also notes the need for a vigorous research program for information warfare defense, especially regarding the global information grid (GIG). However, the research fields that they identify do not address the research needs of the NIAP. For example, they note the need for research in scalable global computing, mobile code security, fault tolerance, and malicious code detection but do not call for research to improve the CCEVS or the NIAP or for research in technologies directly related to them.

D.4.12.4.3 1999 Report of the Defense Science Board on Globalization and Security[140]

This report notes the need for research in the area of what they call "pre-operational integrity" of software systems, but they propose to achieve this goal by the use of red-teaming, use of hackers, and research into smart testing while also calling for the use of

---

[138] OUSD(AT&L), *Report of the Defense Science Board Task Force on Information Warfare Defense,* November 1996, Washington, D.C. document available at http://www.acq.osd.mil/dsb/reports/iwd.pdf.

[139] OUSD(AT&L), *Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations,* 2000 Summer Study, Volume II, March 2001, Washington, D.C. Document available at http://www.acq.osd.mil/dsb/reports/dio.pdf.

[140] OUSD(AT&L), *Final Report of the Defense Science Board Task Force on Globalization and Security,* December 1999, Washington, D.C. Document available at http://www.acq.osd.mil/dsb/reports/globalization.pdf.

the NIAP. They do not call for additional research that would improve the capability of the NIAP to insure pre-operational integrity.

D.4.12.4.4 Information Assurance: Legal, Regulatory, Policy, and Organizational Considerations[141]

This 1999 report by the Joint Staff provides an overview of previous reports and activities as well as missions and roles as they relate to information assurance. The document does discuss the need for cybersecurity research throughout and identifies several arenas where research is needed, but provides no framework, schedule, or prioritization for research.

The following table shows the relationships of the reports to the various issues described.

Table 22. Policy and Reports Regarding NIAP-Related Research

	DoD	Other Federal	NIAP
Need for additional funding and research in cyberdefense		1) Information Security and Privacy Advisory Board 2) Status of the Federal Critical Infrastructure Protection Activities 3) Protecting Information Systems: Supporting the Federal Government and Nation's Critical Infrastructure (GAO, 2003) 4) Cyber Security for Critical Infrastructure Protection (GAO, 2004)	
Need for a vigorous research effort in all areas of information warfare defense	Information Assurance: Legal, regulatory, Policy, and Organizational Considerations	1996 Report of the Defense Science Board on Information Warfare Defense	
Need for vigorous research program outside of NIAP and using non-NIAP techniques	2000 Report of the Defense Science Board on Information Warfare Operations		
Research to insure pre-operational integrity by using NIAP plus other techniques	1999 Report of the Defense Science Board on Globalization and Security		
Research that can be re-purposed to address NIAP needs			1) Status of the Federal Critical Infrastructure Protection Activities 2) Cyber Security for Critical Infrastructure Protection (GAO, 2004)
Research to enable protection of private-sector owned portions of the critical infrastructure		National Strategy to Secure Cyberspace	
Requires Department of Commerce to improve cyber security technology		HSPD 7 (2003)	

D.5 Acquisition

This review is not intended to be an exhaustive review of acquisition policy, but a sample of the primary policies affecting acquisition of IT security products/services.

---

[141] Joint Staff J-6, *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations*, 4th edition, 1999, Washington, D.C.

D.5.1 CSA 1987

In this statute, the Administrator of GSA was charged, under the authority given to him by the Brooks Act,[142] with developing acquisition guidance for Federal Government IT (Federal information resources management) and with ensuring that this guidance was consistent with the standards for computer security promulgated by NIST and made mandatory by the Secretary of Commerce.

D.5.2 OMB Circular A-130

This document contains both general IT acquisition policy, and policy specific for IT security. For the general IT acquisition policy, OMB directs agencies to use competition and to maximize their return on investment, as well as structuring major IT systems into segments to reduce risk, promote flexibility and interoperability, as well as other factors.

For policy specific to IT security, and consistent with and implementing the requirements detailed in the CSA, OMB directed Commerce to issue FIPS and guidelines for acquisition, and GSA to provide guidance to Federal agencies to address security issues when acquiring IT. The direction to GSA included development of broad contract vehicles to obtain computer security products and services, as well as provide cost-effective security services to Federal agencies. GSA implemented these requirements by issuing the Federal Information Resources Management Regulation (FIRMR)[143] and the Federal Acquisition Regulations (FAR).[144] These documents provided little in the way of additional guidance other than stating that Federal agencies must comply with OMB Circular A-130 in addressing security considerations in the procurement of IT.

D.5.3 CCA 1996

As described previously, this act repealed the section of the Federal Property and Administration Services Act of 1949 (40 U.S.C. 750, section 111), resulting in rescission of the FIRMR mentioned above. It focused instead on the authority of the Director, OMB, to oversee Federal agency budget and programs in IT capital planning and investments. This oversight intended to use performance and results-based management to ensure appropriate evaluations of Federal agencies' programs, e.g. OMB to ensure that the information security policies, procedures and practices are adequate.[145] It also provided policy direction for the process of acquisition of IT, and designated the Federal Acquisition Regulatory Council as the responsible agency to assure that the process for acquisition of information technology was simple, clear and understandable.

---

[142] 40 USC 759(d), Federal Property and Administrative Services Act of 1949.

[143] 41 CFR Part 201.

[144] FAR Part 30, Acquisition of Information Technology.

[145] CCA, Section 5113, "Performance Based and Results-Based Management." This entire section emphasizes this point.

D.5.4 EO 13011 Federal Information Technology 1996

This EO implements the requirements for IT contained in CCA, along with PRA 1995[146] and GPRA 1993[147]. It reiterated the responsibilities assigned to Federal agency heads for complying with acquisition guidance contained in the FAR and that to be issued by OMB regarding information systems investments. Although CCA repealed the statute underlying GSA's authority for centralized acquisition of IT for the Federal government, the EO directed GSA to recommend methods and strategies for acquisition of IT. No specific mention of computer security or acquisition of security products or services was made in this document.

D.5.5 Federal Acquisition Regulation (FAR) subpart 239.71[148]

This section of the FAR, titled "Security and Privacy for Computer Systems," was set aside to provide direction to Federal agencies on IT acquisitions and the inclusion of information assurance requirements. Although the FAR applies to all Federal departments and agencies, the only direction it currently contains is very general, mentioning CCA and FIPS standards among other documents, with the remainder of the policy focused at DoD and national security systems (described in a little more detail below under DoD policies). There are a number of FIPS standards applicable to all Federal agencies (with the exception of national security systems), but none specifically address acquisition of IA/IA-enabled IT for Federal agencies. NIST has issued guidance for acquisition of IT security products in two special publications.[149] The guidance provided in these documents is not mandatory or binding on the part of Federal agencies, but does provide a basis for agencies to determine what they should acquire.

D.5.6 NTISSP 11 National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products

This policy, applicable only to the national security community, became effective in January 2001 and established a policy that by July 2002, all IA or IA-enabled products purchased by this community must be evaluated and validated by one of three methods: (1) the International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement (Common Criteria); (2) NIAP; or (3) NIST FIPS validation program. It provides for exemptions and deferred compliance. The policy also states that since these products are normally part of a system, along with other products, a solution security analysis be conducted along with the certification and accreditation process, in addition to the evaluation and validation of specific IA/IA-enabled products. There are no requirements that provide for integration of the product evaluation data with C&A of systems using those products.

---

[146] Public Law 104-13, "Paperwork Reduction Act."

[147] Public Law 103-62, "Government Performance Results Act."

[148] 48 CFR Ch. 2 subpart 239.71.

[149] NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, U.S Department of Commerce, August 2000, and NIST SP-800-36, Guide to Selecting Information Technology Security Products, U.S. Department of Commerce, October 2003.

D.5.7 National Defense Authorization Act (NDAA) FY 2001[150]

Section 811 of this Act provided direction to the DoD CIO on mission critical and mission essential IT systems, specifically, directing the revision of DoDD 5000.1 to establish minimum planning requirements for the acquisition of IT systems. This change mandated these systems must be registered with the CIO, that there be an appropriate information assurance strategy, and that certain milestone requirements be adhered to for major automated information systems (MAIS). Additionally, DoD was required to track purchases of IT products or services, in excess of the simplified acquisition threshold, regardless of the method of purchase to ensure compliance with sections 5122 and 5123 of CCA.

D.5.8 E-Gov Act 2002

Among other things, this Act created the Office of Electronic Government within OMB to oversee Federal government efforts in accomplishing e-gov requirements, including ensuring that products/services were acquired appropriately through capital planning and investment control for information technology as required under CCA.[151] It formally chartered the CIO Council, previously created by EO 13011, and designated this group as the principal interagency forum for improving agency practices related to the design, *acquisition*, development, modernization, use, operation, sharing and performance of Federal Government information resources.[152] The Act also authorized heads of Federal agencies to enter into "share-in-savings contracts" for IT and allowed the agencies to retain savings realized by these contracts (with some stipulations).[153] Finally, this act authorized state and local government to acquire IT through federal supply schedules.[154]

D.5.9 FISMA 2002

FISMA has one concern with regard to the acquisition of IT products i.e. a statement concerning the development of standards by NIST. Federal agencies are required to follow the standards and guidelines developed by NIST:

1. To the maximum extent practicable, ensure that standards and guidelines do not require the use of procurement of specific products, including any specific hardware or software;
2. To the maximum extent practicable, ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

---

[150] Public Law 106–398, National Defense Authorization Act, FY 2001. Title VIII, Subtitle B, "Information Technology," Section 811, "Acquisition and Management of Information Technology," 30 October 2000.

[151] PL 107-347, Section 3602, (e)(1).

[152] Ibid, Section 3603.

[153] PL 107-347, section 210.

[154] Ibid, section 211.

3. To the maximum extent practicable, use flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information security products.[155]

D.5.10 National Defense Authorization Act (NDAA) for Fiscal Year 2003

The NDAA for Fiscal Year 2003 included the following statement of policy regarding DoD acquisitions:

> **SEC. 352. POLICY REGARDING ACQUISITION OF INFORMATION ASSURANCE AND INFORMATION ASSURANCE-ENABLED INFORMATION TECHNOLOGY PRODUCTS.**
>
> (a) ESTABLISHMENT OF POLICY.—The Secretary of Defense shall establish a policy to limit the acquisition of information assurance and information assurance-enabled information technology products to those products that have been evaluated and validated in accordance with appropriate criteria, schemes, or programs.
>
> (b) WAIVER.—As part of the policy, the Secretary of Defense shall authorize specified officials of the Department of Defense to waive the limitations of the policy upon a determination in writing that application of the limitations to the acquisition of a particular information assurance or information assurance enabled information technology product would not be in the national security interest of the United States.
>
> (c) IMPLEMENTATION.—The Secretary of Defense shall ensure that the policy is uniformly implemented throughout the Department of Defense.[156]

D.5.11 DoD Policies Regarding Acquisition and Information Assurance

The DoD has been the most active of the Federal departments/agencies in recognizing the need for computer security in its systems. Historically, the national security systems (for the most part- the classified systems within the Department) were of the most concern and warranted close scrutiny of the IT products and systems used. There have been a number of mechanisms used by the DoD to ensure the security of products and systems, but for the purposes of this report, only those currently in existence are discussed. The policy for DoD systems is comprehensive and provides significant detail in the acquisition and management of DoD IT systems. The following discussion covers the highlights of the major policies. Additionally, each of the major DoD departments/agencies (including the military services) has issued implementing direction specific to their organization. The details of that level of policy and whether that direction is consistent with DoD policy, sufficient to ensure implementation and actually implemented as intended, will not be addressed in this report, but may be appropriate for another study.

---

[155] Ibid, section 303, para (c)(5), (c)(6), and (c)(7).

[156] Bob Stump National Defense Authorization Act for Fiscal Year 2003, P.L. 107-314.

D.5.11.1 DFAR (Defense Federal Acquisition Regulations) June 2004[157]

This regulation codified the policy for national security DoD IT systems that mandated the provision of information assurance for IT, including the requirement for IA/IA-enabled products to be evaluated and validated by the NIAP.

D.5.11.2 DODD 5000.1 The Defense Acquisition System[158]

This directive instructed DoD acquisition managers to address information assurance for DoD systems including weapons systems, C4ISR systems and other IT systems. It referred to DoDD 8500.1 for more detailed information (see below).

D.5.11.3 DoDI 5000.2 Operation of the Defense Acquisition System[159]

This instruction stated that contracts for awards of mission-critical or mission-essential IT systems cannot be awarded until the DoD CIO has determined that the system has an appropriate information assurance strategy. This was done as part of the structured acquisition process for DoD IT systems.

D.5.11.4 DoDD 8000.1 Management of DoD Information Resources and Information Technology[160]

This directive provided the definitive policy to DoD departments/agencies on how they are to manage their IT systems. It included direction to include information assurance requirements during functional process reengineering, outsourcing and information systems design prior to acquisition of new or redesign of existing IT systems.

D.5.11.5 DoDD 8500.1 Information Assurance[161]

This directive provided the definitive policy to DoD departments/agencies on how information assurance will be addressed in DoD IT systems. It reiterated that IA requirements will be addressed in the acquisition of IT systems, including the requirement for all IA/IA-enabled systems to comply with NSTISSP 11 requirements for evaluation and validation. Although NSTISSP 11 applies to national security systems, this directive extended the requirement to all DoD IT systems whether they are national security systems or not.

D.5.11.6 DoDI 8500.2 Information Assurance Implementation[162]

This instruction provided implementation direction for the policies laid out in the companion directive mentioned previously. It provided details on how NSTISSP 11

---

[157] 18 48 CFR Parts 239 and 252.

[158] Department of Defense Directive 5000.1, "The Defense Acquisition System," 12 May 2003.

[159] Department of Defense Instruction 5000.2, "Operation of the Defense Acquisition System," 12 May 2003.

[160] Department of Defense Directive 8000.1, "Management of DoD Information and Information Technology," with Change 1, 20 March 2002.

[161] Department of Defense Directive 8500.1, "Information Assurance," 24 October 2002.

[162] Department of Defense Instruction 8500.1, "Information Assurance Implementation," 6 February 2003.

would be implemented by the DoD components for IA/IA-enabled systems and the use of protection profiles and security targets by vendors in the acquisition process.

D.6 Analysis of Policies by Community

Using the communities of interest described in the previous chapter, the policies were analyzed to determine what policies applied to what communities to get an understanding of the complexities of the policy relationships. The numeric results of this analysis are presented at Table 23. What the table does not show is the potential overlaps in communities of interest where policies intended for different communities are applicable. An example of this overlap would be DoD, which exists as a Federal department, a member (and the executive agent) for the National Security Community, and has elements that are also members of the Intelligence Community. Since the focus of this study is on the Federal government, the communities of interest of state, local and tribal, as well as the private sector, were not addressed. Also included in this analysis, were policy requirements specific to particular activities of interest, specifically NIST, NSA, and the NIAP.

Table 23. Policy Requirements by Community of Interest

Stakeholder Source	Number and Type of Policy Requirements
Federal Community	33 requirements (IA, Acquisition, Certification Accreditation, Standards/Guidelines, CIP, & Reporting)
National Security Community	19 unique requirements (IA, Acquisition, Certification & Accreditation, and Reporting)
DoD	50 unique requirements (IA, Acquisition, CIP, Trusted Computer Systems, Certification & Accreditation, Protection Profiles & Standards)
Intelligence Community	2 unique requirements (IA, Certification & Accreditation)
NIST	14 unique requirements (IA, Standards/Guidelines)
NSA	13 unique requirements (Acquisition, Trusted Computer Systems, Evaluated Products, Protection Profiles, standards/guidelines)
NIAP	15 unique requirements (General)

Table 24 shows the mix of requirements that may be applicable to NIAP evaluated products.

Table 24. NIAP Requirements Matrix

NIAP Requirements	Cybersecurity/Information Assurance/Information Security	Standards/Guidelines	Education & Training	Research	Acquisition	System Certification & Accreditation	Product Evaluation
Statutes							
NBSA/NIST Act (1901/1988/2002)	■	■					
NSA (1947)		■	■				
CSA 1987 (1988)	■	■	■	■	■		
PRA 1980/1995	■	■			■		
NTTAA (1995)		■			■	■	■
CCA (1996)	■	■	■		■		
DIAP (2001)	■						
GISRA (2001)	■	■	■		■		
E-GOV ACT (2002)			■	■	■		
FISMA (2002)	■	■	■	■			
HSA (2002)	■						
CSR&DA (2002)	■			■			
NDAA (2003)	■						■
Treaties & Other International Agreements							
CC-CEM 97/017 (1997)							
Strategies							
NS for Homeland Security (2002)	■						
NS for Physical Protection of CI/KA (2003)	■	■					
NS to Secure Cyberspace (2003)	■	■	■	■	■	■	■
EOP/Federal Policy							
EO 12333		■					
EO 12958		■					
EO 13010	■						
EO 13011 (1996)	■		■		■		
E0 13231 (2001)	■		■				
EO 13355 (2004)	■	■					
NSD 42 (1990)	■						
PDD 63 (1998)	■			■			
HSPD 7 (2003)	■			■			
FAR Part 39					■		
5 CFR Part 930 (2004)(Info Sec Resp for Employees who Manage or Use Federal IS)	■	■	■				
15 CFR Part 287 (2000) (Guidance on Conformance Assessment Activities)		■			■	■	■
48 CFR Parts 239 & 252 (DFARS)	■				■		
OMB Circ A-119 (1998)		■			■		■
OMB Circ A-130 (2000)	■	■	■		■	■	
OMB M-00-07	■						
OMB M-01-08 (GISRA) (2001)	■	■	■			■	
OMB M-03-19 (FISMA) (2003)	■	■	■		■	■	
OMB M-04-15 (HSPD7) (2004)	■	■		■	■		
OMB M-04-25 (FISMA) (2004)	■	■	■		■	■	
National Security Systems Issuances							
NSTISSP 6 (1994)(C&A for NSS)	■	■				■	
NSTISSP 11 (2003)(Acquisition of IA & IA-enabled Products)	■	■			■		■
NSTISSD 501 (1992)(Training for Infosec Prof)	■	■	■				
NSTISSD 502 (1993)(NSS Security)	■	■					
NSTISSI 1000 (2000)(NIACAP)	■	■				■	
NSTISSI 4011(1994)(Training Std for INFOSEC Professionals)	■	■	■			■	
CNSSI 4012(2004)(IA Trng Std for SSMs)	■	■	■		■	■	■
CNSSI 4013(2004)(Trng Std for SAs)	■	■	■		■	■	■
CNSSI 4014(2004)(Trng Std for ISSOs)	■	■	■		■	■	■
CNSSI 4015(2000)(Trng Std for System Certifiers)	■	■	■			■	
NSTISSAM INFOSEC/2-00	■	■			■		■
IC Policy							
DCID 6/3 (1999)(Policy & Manual)	■	■	■	■		■	
DoD Issuances							
DoDD 4630.5 (Interop & Supt of IT & NSS)(2004)	■	■			■	■	
DoDD 5000.1 (Defense Acquisition)(2003)	■	■			■		
DoDD 5000.2 (Ops of Def Acquisition)(2003)	■	■			■		
DoDD 5160.54 (CAAP/CIP)(1998)	■	■		■			
DoD 5200.40 (DITSCAP) (1997)	■	■	■		■	■	
DoDD 5215.1 (1982)(CSEC)	■	■		■	■		■
DoDD 8000.1 (Mgmt of DoD IRM & IT)(2002)	■	■	■		■		
DODD 8100.1 (GIG Policy)(2002)	■	■			■		
DoD 8500.1 (IA) (2002)	■	■	■	■	■	■	■
DoDI 8500.2 (IA Impl)(2003)	■	■	■		■	■	■

NIAP Requirements	Cybersecurity/Information Assurance/Information Security	Standards/Guidelines	Education & Training	Research	Acquisition	System Certification & Accreditation	Product Evaluation
DoDD O-8530.1M (CND) (2003)	■	■	■			■	
DODI 8551.1(Ports, Protocol Mgmt)(2004)	■	■					
DODD 8570.1(IA Trng, Certif Workforce Mgmt)(2004)	■	■	■		■		
DoDI 8580.1 (IA in Def Acq Sys)	■	■			■	■	
CJCSI 6211.02B (DISN Policy etc)(2003)	■	■	■			■	
CJCSI 6510.01D (2004)(IA CND)	■	■	■		■	■	■
NIST Issuances							
FIPS 112(1985)(Password Usage)\	■	■					
FIPS 113(1985)(Computer Data Authentication)	■	■				■	
FIPS 181(1993)(Automated Password Generator)	■	■				■	
FIPS 185(1995)(Escrowed Encryption Std)	■	■				■	
FIPS 186-2(2000)(Digital Signature Std)	■	■				■	
FIPS 188(1994)(Std Security Label)	■	■					
FIPS 190(1994)(Adv Auth Tech Alt)	■	■				■	
FIPS 191(1994)(Analysis of LAN Security)	■	■				■	
FIPS 196(1997)(Auth using PKI)	■	■				■	
FIPS 197(2001)(AES)	■	■				■	
FIPS 198(2002)(Keyed-HMAC)	■	■				■	
FIPS 199(2003)(Security Categorization of Federal Info & Info Systems)	■	■				■	
NIST SP 800-12(1995)(Intro to Computer Security)	■	■	■		■		
NIST SP 800-14(1996)(Principles&Practices fo Securing IT Systems)	■	■	■		■	■	
NIST SP 800-16 (1998) ITS Training Rqmts	■	■	■		■	■	
NIST SP 800-18(1998)(Developing Security Plans for IT Systems)	■	■	■		■	■	
NIST SP 800-21(1999)(Implementing Cryptography in the Federal Government	■	■			■		■
NIST SP 800-23 (2000)(Security Assurance & Acqui/Use of Tested/Evaluated Products	■	■			■		■
NIST SP 800-26(2001)(Security Self-Assessment Guide for IT Systems)	■	■	■			■	
NIST SP 800-27revA(2004)(Engineering Principles for IT Security)	■	■			■	■	■
NIST SP 800-30(2002)(Risk Management Guide for IT Systems)	■	■				■	
NIST SP 800-31(2001)(IDS)	■	■			■	■	■
NIST SP 800-33(2001)(Underlying Technical Models for IT Security)	■	■					
NIST SP 800-34(2002)(Contingency Planning Guide for IT Systems	■	■	■			■	
NIST SP 800-35(2003)(IT Security Services)	■	■	■		■		■
NIST SP 800-36 (2003)(Selecting Information Security Products)	■	■			■		■
NIST SP 800-37 (2002)(C&A of Federal Systems)	■	■				■	
NIST SP 800-40(2002)(Security Patches)	■	■					
NIST SP 800-41(2002)(Firewalls & FW Policy)	■	■			■	■	■
NIST SP 800-42(2003)(Network Security Testing)	■	■				■	
NIST SP 800-44(2002)(Securing Public Web Servers)	■	■				■	
NIST SP 800-45(2002)(Email Security)	■	■	■		■	■	■
NIST SP 800-47(2002)(Interconnecting IT Systems)	■	■				■	
NIST SP 800-50 (2003) IT Security A&T Program)	■	■	■				
NIST SP 800-53 (2005)(Rec Security Controls)	■	■			■	■	
NIST SP 800-55(2003)(Security Metrics for IT)	■	■			■	■	
NIST SP 800-59(2003)(ID IS as a NSS)	■	■			■	■	■
NIST SP 800-60(2004)(Mapping Types of Info & IS to Security Categories)	■	■				■	
NIST SP 800-63rev1.0.1(2004)(Electronic Authentication Guideline	■	■			■	■	■
NIST SP 800-64 rev 1(2004)(Security Considerations in IS Dev Life Cycle)	■	■			■	■	■
NIST SP 800-65(2005)(Integrating Security into the Capital Planning & Investment Control Process)	■	■			■		
National/International Standards							
ISO/IEC 65 (1996)		■					
ISO 17799 (2000)(Information Security Management	■	■	■			■	
CC-CEVS (2004)(ISO/IEC 15408)v2.2	■	■					■
CCArr (2000)	■	■					■

D.7 Additional Statutes of Interest

In general, the Federal Government does not directly regulate the security of non-government computer systems. However, there are three significant exceptions of interest. The Federal Government does require certain information held on non-government systems to be protected against unauthorized access and disclosure, primarily, but not exclusively, out of privacy considerations. To date, this requirement has been limited to customer financial information (Gramm-Leach-Bliley Act of 1999 (GLB Act)), corporate financial information (Sarbanes-Oxley Act of 2002 (SOX Act)), and medical information (Health Insurance Portability and Accountability Act of 1996 (HIPAA)). A number of regulatory agencies have authority for developing, promulgating, and enforcing standards for financial information. SOX Act requires public companies to certify the accuracy of their internal financial controls. The Securities and Exchange Commission (SEC) has authority to develop standards and enforce these regulations. The Secretary of Health and Human Services has authority under HIPAA to develop and enforce standards for medical information. The following discussion provides more detail on the statutes mentioned and how they contribute to cybersecurity within the private sector.

D.7.1 Gramm-Leach-Bliley Act of 1999 (GLB Act)[163]

Title V, Subtitle A of the Gramm-Leach-Bliley Act addresses privacy of consumer's financial information requiring agencies who have authority in the financial services area (listed below) to establish appropriate standards for financial institutions to: (1) insure the security and confidentiality of customer records and information, (2) protect against any anticipated threats of hazard to the security or integrity of such records and (3) to protect against unauthorized access to or use of these records that could result in harm or inconvenience to a customer. The Act directs Federal functional regulators, the Treasury Secretary, and the Federal Trade Commission (FTC), in consultation with State insurance authorities, to prescribe regulations necessary to carry out the purposes of the Act, making every effort to assure such regulations are consistent and comparable.[164] The FTC issued its final rule on the standards for safeguarding customer information in 2002, and provided additional guidance to businesses to which these rules apply.[165] The rule required all financial entities subject to FTC's jurisdiction to develop, implement and maintain comprehensive information security programs, appropriate to the size and scope of the organization. One element of each program is to identify risks to the security, confidentiality, and integrity of customer information in information systems, including network and software design, as well as information processing, storage, transmission and disposal. Other agencies with regulatory authorities have issued similar rules. The net effect of this activity is that almost the entire financial services industry is required to

---

[163] P.L. 106-102, 15 U.S.C. sect 6801, et seq, Title V-Privacy, Subtitle A, "Disclosure of Nonpublic Personal Information," 12 November 1999.

[164] Information regarding these regulations is available at the following web sites: http://www.keytlaw.com/Links/glbact.htm, http://www.ftc.gov/privacy/glbact/index.html.

[165] 16 CFR Part 314, "Standards for Safeguarding Customer Information," 23 May 2002.

provide adequate security over its information systems to ensure compliance with this Act.

D.7.2 Sarbanes-Oxley Act of 2002[166]

Section 404 of the Sarbanes-Oxley Act is being widely interpreted in the legal, accounting and information assurance communities to require all publicly held companies to demonstrate due diligence in the disclosure of financial information and implement appropriate internal controls and procedures to communicate, store and protect that data. Public companies are also required to protect these controls from internal and external threats and unauthorized access, including those that could occur through online systems and networks. ISO 17799[167] is the recommended standard for information security for public companies to which this statute applies. The Cyber Security Industry Alliance (CSIA), the Information Systems Audit and Control Association (ISACA) and the Computer Security Institute (CSI), among others, have recognized the impact of this statute and authored papers or conducted studies addressing issues in this area. The Public Company Accounting Oversight Board (PCAOB), created by the statute to provide oversight for the implementation of this statute, has issued a number of standards and rules, approved by the SEC. [168] The most recent CSI/FBI Computer Crime and Security Survey added a question concerning the effect of this statute on information security activities that CSI will continue to track through annual surveys.[169]

D.7.3 Health Insurance Portability and Accountability Act of 1996

HIPAA imposes stringent requirements on health care providers and others to protect medical information. "Wrongful disclosure of individually identifiable health information" is a criminal offense. HIPAA requires safeguards on the part of anyone who maintains or transmits health information to ensure the integrity and confidentiality of the information and protect against any reasonably anticipated "(i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information…."[170] HIPAA does not distinguish between public and private sector organizations in imposing these requirements; in fact, it is comprehensive in its scope Federal, state and local entities that have a need to collect health information on individuals are included, as well as private sector hospitals, health care organizations and insurance companies. All are required to provide protection for individually identifiable health information. The Department of Health and Human Services (DHHS) published

---

[166] Public Law 107-204, 116 stat. 745, Section 404, "Management Assessment of Internal Controls," H.R. 3763, "Sarbanes-Oxley Act of 2002," 24 July 2002.

[167] ISO 17799, Information technology. Code of practice for information security management, First Edition, 2000-12-01.

[168] Web site address is www.pcaobus.org.

[169] CSI. "2004 CSI/FBI Computer Crime and Security Survey", 2004. report available at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf.

[170] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, §1173(d)(2).

the Privacy Rule in 2002[171] and the Security Rule in 2003,[172] with compliance to begin in April of 2003. The fact that a Security Rule was part of this implementation reinforces the connection between Security and Privacy and provides additional incentive for organizations having this type of information to address their security issues in a more general sense. As with the GLB Act, this statute covers a spectrum of organizations in the affected medical health services industry, thereby mandating information security for another large group of public and private sector entities.

[171] DHHS, "Standards for Privacy of Individually Identifiable Health Information," 45 CFR Parts 160 and 164, 14 August 2002.

[172] DHHS, "Heath Insurance Reform: Security Standards," 45 CFR Parts 160, 162, and 164, 20 February 2003.

Annex F NIAP Historical Data

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. The NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under PL 100-235 (Computer Security Act of 1987). The partnership combines the extensive IT security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

The long-term goal of the NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, the NIAP seeks to:

- Promote the development and use of evaluated IT products and systems;
- Champion the development and use of national and international standards for IT security;
- Foster research and development in IT security requirements definition, test methods, tools, techniques, and assurance metrics;
- Support a framework for international recognition and acceptance of IT security testing and evaluation results; and
- Facilitate the development and growth of a commercial security testing industry within the U.S.

The NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) is a national program for the evaluation of information technology products for conformance to the International Common Criteria for Information Technology Security Evaluation (ISO/IEC Standard 15408, commonly referred to as the Common Criteria (CC)). The CC represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. In the early 1980's the Trusted Computer System Evaluation Criteria (TCSEC) was developed in the United States. In the following decade, various countries began initiatives to develop evaluation criteria that built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT in general. For example, The European Commission published the information Technology Security Evaluation Criteria (ITSEC) and Canada published the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC). The U.S. government published the Federal Criteria for Information Technology Security (FC).

Table 25 below is a chronology of computer security documents and events that preceded the CCEVS and the NIAP.

Table 25. Chronology of Computer Security Documents and Events

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
10/67	Defense Science Board	Task Force assembled to address computer security safeguards to protect classified information in remote-access, resource-sharing computer systems. Report later issued in 02/70	
02/70	U.S. DoD (OSD)	Security Controls for Computer Systems, Report for Defense Science Board Task Force on Computer Security, a RAND Report that made a number of policy and technical recommendations to reduce threat of compromise of classified information processed on remote-access computer systems	
10/72	U.S. DoD (AFSC)	Computer Security Technology Study, prepared by James P. Anderson & Co. for the Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC). Developed solution approaches to technical problems associated with controlling flow of information in resource and information sharing computer systems	
01/73	U.S. DoD	DoD 5200.28M, ADP Computer Security Manual-- Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource Sharing ADP Systems responded to DSB recommendation to establish uniform DoD policy, security requirements, administrative controls and technical measures to protect classified information processed by DoD computer systems. • Established COMPUSEC principles • Stated that security testing and evaluation procedures would be published later (Orange Book) • Laid groundwork for *Orange Book*	
1977	U.S. DoD	DoD Computer Security Initiative created under auspices of the Under Secretary of Defense for Research and Engineering to focus DoD efforts addressing computer security issues.	
1977-1980	National Bureau of Standards (NBS) Later NIST	"Audit and Evaluation of Computer Security," NBS Special Publication #500-19, October 1977. "Processors, Operating Systems and Nearby Peripherals: A Consensus Report," in Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, NBS Special Publication #500-57, MD78733, April 1980 • Began effort to define problems and solutions for building, evaluating and auditing secure computer systems • Held invitational workshops on subject of audit, and evaluation of computer security	
1979	U.S. DoD	Proposed Technical Evaluation Criteria for Trusted Computer Systems, published in support of the DoD Computer Security Initiative. Authored by MITRE Corporation. • Outgrowth of NBS workshop findings and recommendations	
06/79	U.S. DoD	DoD 5200.28M, ADP Computer Security Manual-- Techniques and Procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource Sharing ADP Systems, with 1st Amendment	
01/81	U.S. DoD	DoD Computer Security Center formed to expand on work started by DoD Computer Security Initiative. Goal: To encourage widespread availability of trusted computer systems	
10/82	U.S. DoD	DoD 5215.1, Computer Security Evaluation Center established DoD Computer Security Evaluation Center (CSEC) to provide policy and assign responsibilities for technical evaluation of computer system and network security.	CSEC
08/83	U.S. DoD	CSC-STD-001-83, Trusted Computer System Evaluation Criteria, National Computer Security Center (NCSC) • Layered approach to security "strength" rating • Oriented for custom software running on mainframe systems • Difficult to apply to networks and databases, interpretations provided. • Evaluations paid for by Government	TCSEC or *Orange Book*

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
12/85	U.S. DoD	DoD Computer Security Center renamed: The National Computer Security Center (NCSC) • Goal: To encourage widespread availability of trusted computer products for use on systems that processed classified or other sensitive information • Approach to produce generic requirements that could be used by vendor to produce trusted products and would serve as standardized criteria for evaluating the trust classes of those products	NCSC
12/85	U.S. DoD	DoD 5200.28-STD, Trusted Computer System Evaluation Criteria, National Computer Security Center (NCSC) Superseded CSC-ST-001-83 • Defined seven security levels for trusted hardware, software and data components of a system • Goal: To provide a level of measurement and guidance in designing secure systems • TCSEC Standard served to: 1) Provide product manufacturers with a standard of security features to build into products; 2) Provide DoD components with metric to evaluate how much trust could be placed in an automated information system; and 3) Provide a basis for specifying security requirements in acquisition specifications • Under the Trusted Product Evaluation Program (TPEP), vendors approached NSA with COTS products and requested evaluation Evaluators under TPEP used TSEC and its interpretations to access how well products met requirements for targeted rating • Designed for government installations not corporate networks • Designed for standalone systems • Appendix A: Commercial Product Evaluation Process	TCSEC or *Orange Book*
12/85	U.S. OMB	Office of Management and Budget, Appendix III to OMB Circular No. A-130, Security of Federal Automated Information Resources, • Required that federal agencies assure each system appropriately uses effective security products and techniques consistent with standards and guidance from NIST	
07/87	U.S. DoD	NCSC-TG-005, v1.0, Trusted Network Interpretation of the TCSEC, National Computer Security Center	TNI, Part of Rainbow Series Red Book
01/88	U.S. Congress	Computer Security Act of 1987, Public Law 100-235 (H.R. 145) • Amended the *National Bureau of Standards/NBS Organic Act of 1901, P.L. 56-177 and assigned responsibility to NBS for developing standards and guidelines for federal computer systems, drawing on technical advice and assistance from NSA. *The Omnibus Trade and Competitiveness Act of 1988, P.L. 100-418, changed the name of the National Bureau of Standards (NBS) to the National Institute of Standards and Technology (NIST)	
3/89	NIST/NSA	Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, (Computer Security Act of 1987) Directed NIST to recognize NSA-certified rating of evaluated trusted systems under TCSEC without requiring further evaluation.	
08/90	U.S. DoD	NCSC-TG-011, v1.0, Trusted Network Interpretation Environments Guideline – • Guidance for Applying the TNI, National Computer Security Center	TNI, Part of Rainbow Series Red Book

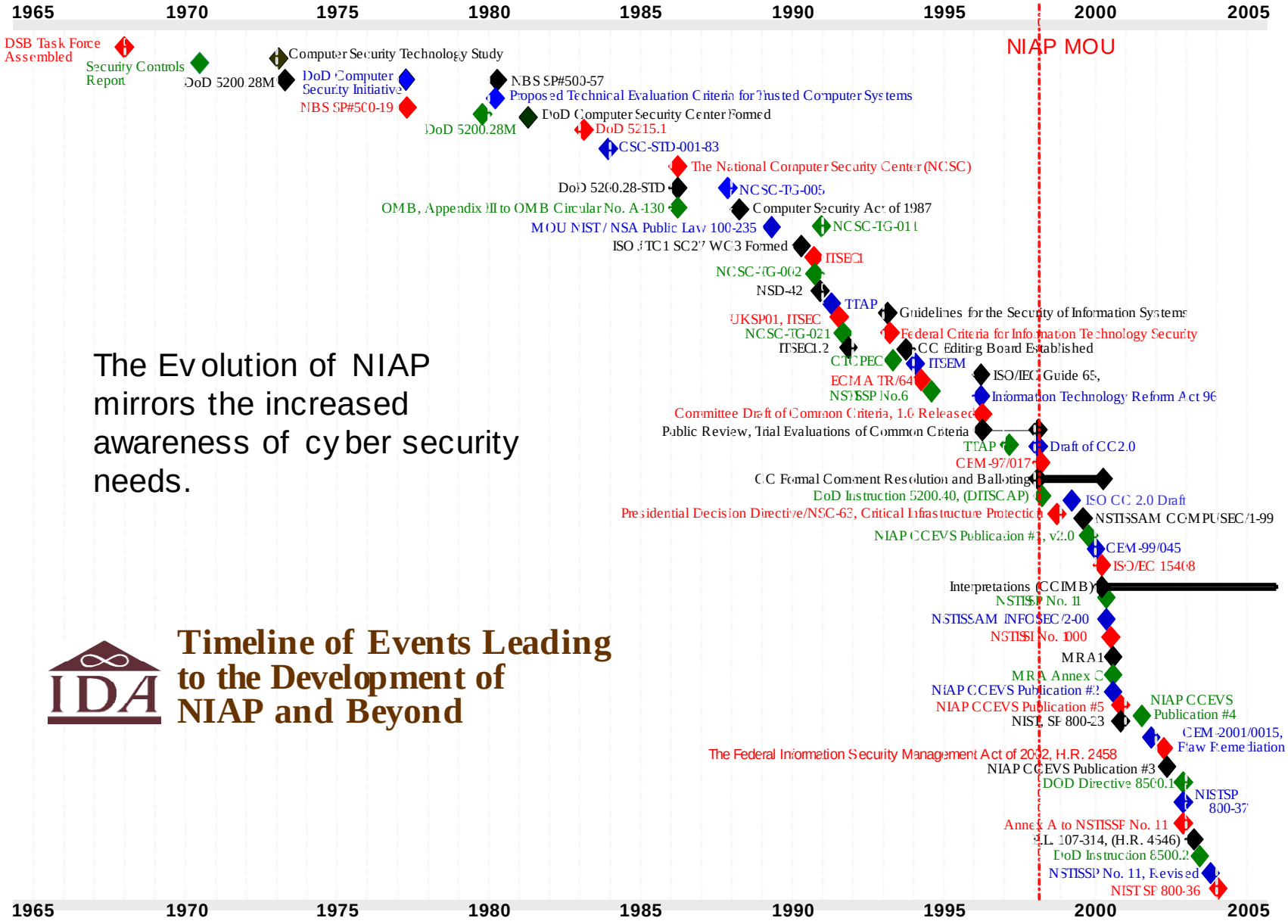
Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
1990	ISO/IEC	JTC1 SC27 WG3 formed (Joint Technical Committee, Information Technology, Subcommittee-27 "Security Evaluation Criteria.")	SC27
05/90	European Communities	Information Technology Security Evaluation Criteria (ITSEC), v1.0 • Commission of the European Communities (to include Germany, France, The Netherlands, United Kingdom)	ITSEC
06/90	U.S. DoD	NCSC-TG-002, Trusted Product Evaluations – A Guide for Vendors, National Computer Security Center	TPEP, Part of Rainbow Series Bright Blue Book
07/90	U.S. National Security Council	NSD-42, National Policy for the Security of National Security Telecommunications and Information Systems, • Outlines that U.S. Government capabilities for securing national security systems against technical exploitation shall be maintained or improved if inadequate... and that a technical base within the government exist to achieve this security and that initiatives with the private sector to maintain, complement or enhance that base and to ensure information security systems security products are available to secure national security systems...	
1991	NIST[CORRECT]	Originated concept of Trust Technology Assessment Program (TTAP) • Alternative approach to emerging Federal Criteria for performing evaluations	TTAP
03/91	U.K. CESG	UKSP01, U.K. IT Security Evaluation Scheme: Description of Scheme, Communications -Electronics Security Group	
04/91	U.S. DoD	NCSC-TG-021, v1.0, Trusted DBMS Interpretation of the TCSEC, National Computer Security Center	Part of Rainbow Series Purple Book
06/91	European Communities	Information Technology Security Evaluation Criteria—Provisional Harmonized Criteria (ITSEC), v1.2, Office for Official Publications of the European Communities, Commission of the European Community (DG/XIII/C.4) • Commission of the European Communities • Originated from national security certification criteria from Germany's BSI, France's SCSSI and the Netherlands NLNCSA • Evaluations paid for by Vendor	ITSEC
11/92	OECD	Guidelines for the Security of Information Systems, 1992, Organization for Economic Cooperation and Development	
12/92	U.S. NIST and NSA	Federal Criteria for Information Technology Security, v1.0, Vols. I and II • Intended as replacement to *Orange Book*	Federal Criteria
01/93	Canadian CSE	The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Canadian System Security Centre, Communications Security Establishment, v3.oe • Canadian Communication Security Establishment • Considered a combination of ITSEC and TCSEC approaches	CTCPEC
06/93	CC Sponsoring Organizations	CC Editing Board established	CCEB
09/93	European Communities	Information Technology Security Evaluation Manual – Provisional Harmonized Methodology, (ITSEM), Commission of the European Community	ITSEM
12/93	ECMA	Secure Information Processing Versus the Concept of Product Evaluation, Technical Report ECMA TR/64, European Computer Manufacturers' Association	ECMA TR/64

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
04/94	U.S. CNSS	NSTISSP No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems Required that all federal government departments and agencies establish and implement programs that mandate certification and accreditation of national security systems	
1996	ISO	ISO/IEC Guide 65, General Requirements for Bodies Operating Product Certification Systems	
1996	U.S. Congress	Information Technology Reform Act of 1996 (Part of the National Defense Authorization Act for Fiscal Year 1996) • Requires that OMB oversee the development and implementation of standards and guidelines pertaining to Federal computer systems by the Department of Commerce through NIST.	
01/96	CCEB	Committee draft of Common Criteria, 1.0 released • CPCTEC, ITSEC and TCSEC combined to form version 1.0 of Common Criteria	CC
01/96-10/97	--	Public review, trial evaluations of Common Criteria	CC
1997	U.S. NSA and NIST	Trust Technology Assessment Program (TTAP) established, along with TTAP Oversight Board and TTAF Evaluation Facilities (TEF) • Transitioned commercial evaluation program into private sector • Commercial organizations allowed to conduct security evaluations of COTS computer security products using TCSEC • TTAP scheme used during the transition to the NIAP/Common Criteria Evaluation Scheme (NIAP/CCEVS)	TTAP
10/97	CCIMB	Committee draft of CC, 2.0 beta released (Interim Arrangement—Canada, United Kingdom, United States)	CC
11/97	CEMEB	CEM-97/017, Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and General Model, v0.6 • Outlined universal principles of evaluation	CEM Part 1
10/97-12/99	CCIMB with ISO/IEC JTC1 SC27 WG3	Formal comment resolution and balloting conducted (Full Arrangement—Canada, France, Germany, United Kingdom, United States, Australia, New Zealand).	CC
12/97	U.S. DoD	DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), • Outlines IT security certification and accreditation process • Addresses integrity analysis of integrated products (COTS, GOTS or Non-Developmental Item (NDI)) • Looks at system security test and evaluation	DITSCAP
05/98	U.S. Office of the President	Presidential Decision Directive/NSC-63, Critical Infrastructure Protection • Required that each department and agency of the Federal Government be responsible for its own critical infrastructure, especially its cyber-based systems	
1999	CCIMB	Committee draft of CC, 2.0 revised released - Version became known as ISO 15408	CC
03/99	U.S. CNSS	NSTISSAM COMPUSEC/1-99, Advisory on the Transition From the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation,	

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
05/99	NIST/NSA	NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Organization, Management and Concept of Operations) Scheme Publication #1, v2.0 • National Information Assurance Partnership established (NIAP) • the NIAP is the collaborative effort of NIST and NSA • Serves as interface to Common Criteria • the NIAP Validation Body provides technical guidance to testing laboratories and validates IT security evaluations for conformance to the Common Criteria	NIAP
08/99	CEMEB	CEM-99/045, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, v1.0	CEM Part 2
12/99	ISO/IEC	ISO/IEC 15408, Information Technology – Security Techniques – Evaluation Criteria for IT Security, Parts 1-3 released (ISO/IEC SC 27) • First international information technology security evaluation criteria standard.	CC Parts 1-3
12/99 (Ongoing)	CCIMB	(Ongoing) Respond to "Requests for Interpretations," issue "Final Interpretations," incorporate Final Interpretations	CC
01/00	U.S. CNSS	NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, • Required that acquisition of all COTS IA and IA-enabled IT products be limited to those evaluated in accordance with the Common Criteria or the NIAP Evaluation and Validation Program or the NIST FIPS validation program	
02/00	U.S. CNSS	NSTISSAM INFOSEC/2-00, Advisory Memorandum For the Strategy For Using the National Information Assurance Partnership (NIAP) For the Evaluation of Commercial Off-The-Shelf (COTS) Security Enabled Information Technology Products. • Addressed evaluation procedures and processes • Outlined that the NIAP would review laboratory report to determine if analysis was consistent with Common Criteria requirements • Advised that government customers would look to the NIAP program for security and security-enabled COTS IT product evaluation requirements	
04/00	U.S. CNSS	NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), • Provided guidance on how to implement NSTISSP No. 6	NIACAP
05/00	Multiple	1. Common Criteria, Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology; (Common Criteria Recognition Agreement signed (Harmonized Arrangement---Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom, United States, later Israel and Sweden) • Sought to ensure evaluations are performed at consistent standards • Improve availability of evaluated products • Eliminate burden of multiple evaluations • Continuously improve evaluation process • Merged members of prior arrangements, members of the full CC arrangement with members of the ITSEC arrangement • Major goal of CC: To work with ISO Joint Technical Committee, Subcommittee 27 (JTC1 SC27 WG3) to make CC an international ISO Standard 2. Common Criteria, Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology, Annex C • Outlined requirements for certification/validation body	CCRA

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
05/00	NIST/NSA	NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Validation Body Standard Operating Procedures), Scheme Publication #2, v1.5	NIAP
08/00	NIST/NSA	NIAP, NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to Sponsors of IT Security Evaluations) Scheme Publication #5, v1.0	NIAP
08/00	NIST	NIST, SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, Recommendations of the National Institute of Standards and Technology, • Instructs federal agencies to give substantial consideration in IT procurement and deployment to products that have been evaluated and tested against security specifications and requirements, such as NIST protection profiles based on the Common Criteria and ISO/IEC 15408	
03/01	NIST/NSA	NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to CCEVS Approved Common Criteria Testing Laboratories) Scheme Publication #4, v1.0	NIAP
08/01	CEMEB	CEM-2001/0015, Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Supplement: ALC_FLR – Flaw Remediation, v1.0	CEM Part 2 Supplement
2002	U.S. Congress	The Federal Information Security Management Act of 2002, H.R. 2458 • Requires that each agency conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices	FISMA
02/02	NIST/NSA	NIAP, NIAP Common Criteria Evaluation and Validation Scheme for Information Technology Security, (Guidance to Validators of IT Security Evaluations) Scheme Publication #3, v1.0	NIAP
10/02	U.S. DoD	DoD Directive 8500.1, Information Assurance, • Required that all IA or IA-enabled hardware, firmware or software products comply with NSTISSP No. 11	
10/02	NIST	NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems • Discusses use of standards such as the CC, ISO/IEC 15408 for component product-level evaluations, but further suggests an evaluation of the integrated system to ensure greater security	
10/02	U.S. CNSS	Annex A to NSTISSP No. 11, Deferred Compliance Authorizations (DCAs)	
12/02	U.S. Congress	National Defense Authorization Act for Fiscal Year 2003, Subtitle F – Information Technology, Section 352, P.L. 107-314, (H.R. 4546) • Required that acquisition of DoD IA and IA-enabled products be limited to evaluated products	
05/02	U.S. DoD/USAF	AF-CIO Policy Memorandum 02-14; Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products • Required that all government acquired COTS/GOTS IA and IA-enabled products be evaluated against the Common Criteria or the NIAP Evaluation and Validation Program or the NIST FIPS validation program	
02/03	U.S.DoD	DoD Instruction 8500.2, Information Assurance (IA) Implementation • Required that protection profiles be developed in accordance with the Common Criteria within the NIAP framework • NSA will generate protection profiles • Acquisition of GOTS IT products is limited to products evaluated by NSA, COTS IT products are limited to those evaluated through the Common Criteria, the NIAP Evaluation and Validation Program or FIPS	

Date	Organization	Document/Standard /Project-Program/Legislation	Short Name
06/03	U.S. CNSS	NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, Revised • Set 07/01/02 deadline for implementation of the requirement that acquisition of all COTS IA and IA-enabled IT products be limited to those evaluated in accordance with the Common Criteria or the NIAP Evaluation and Validation Program or the NIST FIPS validation program	
10/03	NIST	NIST SP 800-36, Guide for Selecting Information Technology Security Products, Recommendations of the National Institute of Standards and Technology • Indicates that organizations should consider acquisition of IT security products that have been evaluated against specifications and requirements such as protection profiles based on ISO/IEC 15408 and the Common Criteria	



The Evolution of NIAP mirrors the increased awareness of cyber security needs.

Timeline of Events Leading to the Development of NIAP and Beyond

Annex G Software Tools for Security Analysis and Proactive Defense

This annex discusses the potential application of tools to support security evaluations. It first notes that most vulnerabilities are caused by a few well-known implementation errors, and discusses other reasons why tools are being increasingly applied to the problem of developing secure software, for security analysis and proactive defense. This is followed by a brief overview about tools, discussion of two particular types of tools (static vulnerability identification tools and fuzz testing tools), and a brief discussion of some of the many other kinds of tools available. The next sections demonstrate that the CC does not currently require the tool use, and then explains why tools (properly used) should reduce vulnerabilities in software. This annex concludes with a discussion about the implications of increasing the use of tools to support evaluations.

F.1 Most vulnerabilities are caused by common well-known errors

Most security vulnerabilities are caused by a relatively small set of well-known software implementation errors. In the CERT's vulnerability reports, 9 of 13 advisories in 1998 and at least half of the 1999 advisories involved buffer overflows. An informal 1999 survey on the Bugtraq security mailing list found that 2/3 of the respondents believed buffer overflows were the leading cause of system security vulnerabilities (the remaining respondents identified "mis-configuration"' as the leading cause) [Cowan 1999]. Buffer overflows are an old, well-known problem, yet buffer overflows continue to resurface [McGraw 2000]. [More CURRENT REFERENCES INSERT]

The Open Web Application Security Project (OWASP) has developed "The OWASP Top Ten," which represents a broad consensus of the most critical web application security flaws are. Their list is:

1. invalidated input,
2. broken access control,
3. broken authentication and session management,
4. cross site scripting (xss) flaws,
5. buffer overflows, injection flaws,
6. improper error handling,
7. insecure storage, denial of service, and
8. insecure configuration management. [OWASP 2004]

Gary McGraw has stated that the most common reasons for vulnerabilities are:

1. buffer overflows,
2. race conditions,
3. errors in random number generation,
4. misuse of cryptography, and
5. trust problems (failing to validate input, trusting input too much, and authentication. [FESTA2001]

Books on developing secure software typically identify a set of common errors that produce security vulnerabilities and how to prevent them. [HOWARD2002a] [VIEGA2002] [WHEELER2003]

The Common Criteria's own Common Evaluation Methodology (CEM) implies that certain situations are leading causes of vulnerabilities. The CEM guidance for implementing vulnerability analysis (AVA_VLA) has a long list of common vulnerabilities and mistakes that "should be considered." [CC1999]

Since a relatively small set of vulnerabilities appear to cause most of the security vulnerabilities, it is reasonable to ask if tools could help find some of them to make the process more efficient. There are other reasons to consider tools as well.

F.2 Why Tools?

Several other factors drive the increasing interest in using tools to reduce vulnerabilities, including the following:

1. *Large and increasing code sizes*. In 1990, Windows 3.1 was 2.5 million lines of code; by 2001 Windows XP contained 40 million lines of code. [FESTA2001] Red Hat Linux 7.1 included over 30 million physical source lines of code (SLOC) by 2001, compared to well over 17 million SLOC in version 6.2 of just one year earlier. [WHEELER2002] These massive and ever-increasing sizes make manual review more difficult, and more likely to miss problems, driving developers increasingly towards using tools. Even in popular open source software projects where "all submitted code is inspected by other members of the group." [JACKSON2004]
2. *Time-to-market pressures*. In theory, given enough time, manual reviews could thoroughly examine any product. But time-to-market pressures make time a luxury, driving software development industry to use tools where practical if they wish to reduce vulnerabilities.

F.3 Tool Basics

Many tools are available that attempt to identify and/or counter previously unknown vulnerabilities in a program. Generally these tools can be divided into static tools and dynamic tools:

1. Static tools do not execute the program being evaluated. These tools examine the source code or binary code of the program to counter vulnerabilities. One particular type of static tool is a "vulnerability identification tool," which searches for patterns that suggest vulnerabilities. Other tools can exploit annotations to prove (or fail to prove) some property of the program. Compilers have many built-in checks, and often provide options (or can have them added) to impose stricter requirements on their inputs; these can be used to require the software to have certain quality properties that may reduce the likelihood of security-related flaws. Techniques that prove that a program has or does not have certain properties, using mathematics and certain assumptions, also fit into this category. A vast number of such tools require the program's source code, and cannot be applied effectively without it.
2. Dynamic tools do execute the program being evaluated. These tools may inject malicious input to see what the program does with it, or manipulate the environment to see if the program can handle changes in its environment well, or detect situations strongly suggesting a vulnerability (and then countering it). Many of these tools can be used without source code, but a number essentially require source code because they require the insertion of instrumentation into the source code.

The literature generally suggests that the best approach is to use several different types of tools together. Any specific tool has many limitations, for example, a tool may only find a certain limited class of vulnerabilities, it may work only on a limited set of languages, or it may only work when examining software developed for specific platforms or circumstances. Many tools have significant false positive or false negative rates. As a result, it is often more effective to use a set of different kinds of tools, so that each tool can address other tools' weak points.

Tools are not a panacea. Tools are best considered an adjunct to human review to help make evaluations more cost-effective, instead of considering tools a complete replacement for humans. Other measures, such as performing human review of the software (requirements, design, code, tests) and ensuring that developers understand how to develop secure software, can help counter or uncover problems that the tools cannot. Nevertheless, tools can be a very useful adjunct to human evaluation. For example, Microsoft's "Trustworthy Computing Security Development Lifecycle" includes both static checking tools and fuzz testing, as well as human review [LIPNER2005].
The following sections describe in more detail two specific kinds of tools: static vulnerability identification tools and fuzz testing tools. This is followed by a brief discussion of some of the many other tools available. Specific tools are mentioned as examples, and are not endorsements of any particular tool.

F.4 Static Vulnerability Identification Tools

One type of tool especially relevant to security evaluations are what this report will term "static vulnerability identification tools." These tools are designed to examine source code (or in rare cases, object code) and identify patterns that suggest the presence of a vulnerability. This is in contrast to approaches such as formal methods approaches, which formally prove a particular property based on static analysis (but require careful statement of the property to be proved and assumptions that can be made).

A few papers that examine static vulnerability identification tools, some of which also examine other tools, include:

- [COWAN2003] reviews various vulnerability identification tools released under an open source software license, calling such tools "software auditing" tools.
- [BROADWELL2002] used static source code analysis and software fault injection against some commonly-used applications and concluded that although static tools found many false positives, "when the tool did find an error [it was] extremely useful." They also found that, when comparing static and dynamic approaches, "the strengths of the two types of tools can be combined in mutually advantageous ways."
- [WILANDER2002a] reviews some publicly-available static tools and argues that tools to help clean up vulnerable code are necessary, but that these tools should be "a support during development and code auditing, not [a] substitute for manual debugging and testing." This is because static tools using lexical analysis produce too many false positives, while other static tools produce too many false negatives.
- [NAZARIO2002] reviews several static analysis tools, and reports that they will "never replace a good manual audit of the code," but that such tools can "help improve the state of your code in development or afterwards… the use of two [or

more] tools is recommended… [these tools] help assist you in the auditing process, not automate it." [WILANDER2002b] includes more detail.

- [TEVIS2004] notes that static tools (termed code security checkers) provide an excellent service, though they still need to improve. Tevis reported that most of the current tools are limited to Unix (not Windows or Macintosh), require a significant amount of expert knowledge for use, and that analysis is time-consuming. Tevis claims that such tools cut down only about ¼ to 1/3 of the analysis that needs to be performed, but does not provide justification for these figures. Tevis argues developers should "move into a functional [programming] paradigm" to improve security, however, there is little evidence that developers are willing to radically switch to such an approach, and there is also little evidence that this would really solve the problem.

These tools have both false negative and false positive rates. They have false negatives (there are problems they cannot find); they will only find those problems that match patterns in their pattern database. To be fair, humans can't guarantee that they will find all vulnerabilities either. Many of these tools also have a large false positive rate (they will report code instances as suspicious that are not actually security vulnerabilities), though there is reason to believe these false positives can be reduced as these tools improve their analysis techniques. Often this is a trade-off; tools with fewer false negatives tend to have more false positives, and vice versa. Thus, many of the papers describe these tools as aids to help speed human evaluation (by helping people find the riskiest areas of the software), instead of being replacements for human evaluation.

F.5 Fuzz Testing Tools

One approach for dynamically detecting security vulnerabilities is called "Fuzzing," that is, generating a large number of random test cases and seeing if the program does not crash or hang. The original fuzzing approach had the following characteristics (as defined at the "Fuzz Testing of Application Reliability" website at http://www.cs.wisc.edu/~bart/fuzz/fuzz.html):

1. "The input is completely random. We do not use any model of program behavior, application type, or system description. This is sometimes called black box testing. In the original UNIX studies (1990 and 1995), the random input was simply random ASCII character streams. For our X-Window study (in the 1995 study) and our Windows NT study (2000), the random input included cases that had only valid keyboard and mouse events.
2. Our reliability criterion is simple: if the application crashes or hangs, it is considered to fail the test, otherwise it passes. Note that the application does not have to respond in a sensible manner to the input, and it can even quietly exit.
3. As a result of the first two characteristics, fuzz testing can be automated to a high degree and results can be compared across applications, operating systems, and vendors."

This is an extremely trivial test criterion. Yet several papers demonstrated that many programs could not even pass this trivial criterion. [MILLER1990] [MILLER1995] [FORRESTER2000]

Although it was originally conceived as a trivial measure of reliability, many observers noticed that fuzz testing tended to identify problems that were also security flaws, such as input validation errors and buffer overflows. Thus, people began to use fuzz testing specifically as a security test. In many cases, when used as a security test, truly random data is not created or is not the only possibility; often fragments or random alternatives are used. Also, when used for security, some may not only detect crashes or excessive computation times; they may also instrument try to detect certain common indicators of vulnerabilities (such as unsafe openings of temporary files in a shared directory), or the code may be instrumented to detect some "should not happen" situations (and intentionally crash the application if they occur). However, in all cases fuzz testing does *not* attempt to determine if a program produced a "correct" answer, merely that the program did not have an obvious failure.

For example, in 2004, Michal Zalewski developed in his spare time a simple tool called "mangleme." This tool generates "tiny, razor-sharp shards of malformed HTML [the data format used by web browsers]." Yet this trivial tool managed to find security problems in every web browser it examined, [ZALEWSKI2004a] [ZALEWSKI2004b] including the one that was the basis of the W32.Bofra.E@mm mass-mailing worm. [SYMANTEC2005] [USCERT]

Microsoft defines fuzzing as "structured but invalid [random] inputs to software application programming interfaces (APIs) and network interfaces so as to maximize the likelihood of detecting errors that may lead to software vulnerabilities." In their approach, small tools must be developed specifically for each API and file format, but these tools are small and easy to write. Microsoft recently added fuzzing as a required part of their "security development lifecycle," and reports extremely encouraging results from its use. [LIPNER2005]

Traditional testing approaches often require that a specific test case be developed so that the "correct" answer can be determined before running the test. As a result, relatively few tests are normally created for software compared to the set of possible program inputs. In contrast, fuzz testing does not require knowing the correct answer (nor writing a program to check for correctness). Thus, fuzz testing can check many more possible inputs than is possible in traditional testing approaches. And once a failure occurs, the data that caused the failure can be used to identify the root cause.

There are reasons to believe fuzz testing will become more effective in the future for initial versions of software, unless developers change their development approaches. As processor speeds increase, and the costs of processors go down (enabling more parallelism for the same cost), the number of possible tests fuzz testing can perform goes up. In addition, as the number of paths in a program goes up (due to its increasing size), the number of paths that may have an error that can be detected by fuzz testing goes up as well.

However, fuzz testing does have quickly decreasing returns after it is first used against a given program. Once initial problems are fixed, in most programs it becomes more and more difficult to find new vulnerabilities with the technique. If developers know that fuzz testing will occur, they often devise stronger input validation routines to prevent most invalid data from entering the rest of the program. But these are not problems per se; in

particular, any process that encourages developers to strengthen their input validation routines is likely to be an improvement.

Because fuzz testing has an extremely naïve definition of "failure," there are many security vulnerabilities it cannot detect. Nevertheless, there is evidence that it can be effective as part of a larger process for detecting security vulnerabilities.

F.6 Other Tools

There are a vast number of tools related to security, and more are being developed all the time. Here are a few examples:

1. *Compiler warning flags and style checkers*. Many compilers include built-in warning flags to enforce certain style requirements not necessarily required by the language, and there are also separate tools that can perform such checks. Typically these requirements are imposed as an effort to detect common mistakes, avoid constructs that are often misused or hard to maintain, and to improve understandability/reviewability. By enabling these options, developers can avoid some common errors that in some cases lead to security vulnerabilities. In some cases these checks are added because they often indicate common errors that lead to security vulnerabilities, so the boundary between these tools and static vulnerability identification tools is blurring.
2. *Secure libraries*. Since easily made programming mistakes are the cause of many security vulnerabilities, one approach is to modify existing programming libraries or to create new libraries that are easier to use securely. For example, ISO has begun work on a technical report to define new library functions for the C programming language to simplify development of secure programs.
3. *Languages with improved security properties*. The highly popular C and C++ programming languages are extremely permissive, and require programmers to perform many low-level tasks such as tracking memory. Mistakes in doing so cause many problems; for example, C and C++ are the only languages in widespread use where buffer overflows can occur by default. Developers could choose to use languages where many common mistakes are not possible or far less likely can reduce the number of security vulnerabilities. However, no language can prevent all possible security vulnerabilities. It is unlikely that a blanket requirement to avoid permissive languages would be commercially viable, especially if it were applied at EAL5 or below; there is simply trillions of dollars invested in C/C++ programs, and the expense of rewriting them would be difficult to justify. Also, applications almost always run on some C and/or C++ code, even if the application itself is not written in them, because many critical reused libraries, nearly all language run-times, and nearly all commercial operating system kernels are written in C. Sometimes another language's run-time inhibits some protective measures for C. For example, the GNAT compiler (a popular Ada compiler) uses "trampolines" in its implementation, and must turn off certain protections used by some [Kleen 2004].
4. *Run-time environment countermeasures for common vulnerabilities*. In some cases a platform (such as the operating system or language run-time) can detect the symptoms of a vulnerability or attack, and reduce the damage it can cause. Since

buffer overflows are an especially common security vulnerability, many tools have been developed to detect and counter them at run-time by halting the program (turning a potential complete take-over of a machine into a denial-of-service attack). Examples include StackGuard [COWAN1998], Microsoft's /gs compiler switch [BRAY2002], IBM's Scientific Subroutine Package (SSP) [WILANDER2003], and Red Hat Linux's ExecShield [VANDEVEN2005]. Environmental countermeasures have been developed to counter other vulnerabilities as well, such as for temporary file race conditions [COWAN2001a], format string errors [COWAN2001b], and double-free errors.

5. *Proof-making/checking tools*. Over several decades there have been many efforts to develop tools to support formal methods. Proof-checking tools can confirm the validity of a proof, and proof-making tools can develop some proofs automatically (in practice, often requiring human guidance). In general, applying these tools to source code requires extreme rigor, specialized language subsets, and a commitment to developing source code and the necessary annotations for proof simultaneously.
6. *Standard test suites and vulnerability scanners*. Standard sets of tests can be developed for common product classes (such as firewalls or operating systems). Indeed, network security scanning tools (such as Nessus) that can actually send real attacks (not just check version numbers) already embody a large set of specific security tests, and can be used to determine if a product can withstand attacks that have worked elsewhere. Such test suites can send attacks that have succeeded in the past, as well searching for general issues such as unexpected open ports or cleartext passwords. Such tools are especially useful for regression testing, for example. They are limited, obviously, to the specific items they test for, so they should be supplemented with other tools designed to detect previously unknown kinds of vulnerabilities.

In some cases, it would be possible to impose support for certain tools in a Protection Profile. For example, operating systems could be required to include as buffer overflow run-time environment countermeasure (which could be checked using simple a simple standard test suite), and applications could be required to enable certain compiler options under certain conditions.

F.7 Common Criteria do not require tools

A careful analysis of the Common Criteria shows that while they *permit* the use of tools, they do not *require* the use of any tool. In addition, the Common Criteria's approach to source code inhibits the use of many tools; full source code is only required at EAL5, and none is required below EAL4 in the current version.

The Common Criteria do have some requirements for vulnerability analysis in the family AVA_VLA. The lowest level, AVA_VLA.1, is required at EAL2; the next-lowest level, AVA_VLA.2, is required at EAL4. However, the instructions for performing such evaluations are vague, and do not specifically require any kind of tool use, even when such tools are available and appropriate. A vulnerability analysis is defined by the CEM as a "systemic search," (section 8.10.3.2). The EAL4 CEM work unit 4: AVA_VLA.2-9 provides a list of issues that an evaluator should consider. However, the entire CEM text appears to presume a manual consideration of issues, and manual creation of tests to

prove or disprove the existence of a vulnerability. It certainly does not require the use of tools.

At the higher levels, some of the CC text could be interpreted as supporting the use of tools, but it does not explicitly require them. The higher–level AVA_VLA.3 (required at EAL5) requires a "systematic" search for vulnerabilities; a process using tools might be termed systematic, but a manual systemic process could also meet this requirement so there is no clear requirement for them. The strongest vulnerability analysis requirement, AVA_VLA.4, is required for EAL6 and 7; it requires a justification that the analysis "completely addresses the TOE deliverables" but again does not require the use of tools.

Since some types of tools tend to report a number of false positives, evaluators may have a financial disincentive to use tools to examine potential vulnerabilities. An evaluator can increase profits by merely positing a small set of vulnerabilities (as permitted by the CC), so that only a limited subset of vulnerabilities needs to be considered, instead of using tools as a supplement to their analysis.

In many evaluations, the lack of source code severely restricts tool use, since many tools require access to the source code and/or the ability to rebuild the program. In the Common Criteria, evaluations at EAL3 and below do not require source code, and at EAL4 only a subset of source code is available (as requirement ADV_IMP.1). Access to all of a program's source code is not required until EAL5 (as requirement ADV_IMP.2). Since many evaluations only occur at EAL4 and below (to meet mutual arrangement requirements as well as to reduce costs), the current CC structure makes it difficult to employ tools for most evaluations. Even if the vendor is willing to release all their source code to an evaluator (a common circumstance as long as protective measures are put in place), evaluators cannot consider the whole set since to do so would create an unfair situation between vendors. It is expected that the next revision of the Common Criteria will require all source code at EAL4, but this does not help in lower-level evaluations. See the discussion on source code review for more information.

This is more striking when the actual Common Criteria requirements are compared with people's expectations. All stakeholder classes expected that the NIAP would provide tools and require source code analysis (see section 5, "Testing of Products in Evaluation").

F.8 Tools should reduce vulnerabilities and effort to find them

Tools, when properly developed and used, should detect and/or counter a significant proportion of the most common vulnerabilities. As noted earlier, most vulnerabilities are caused by a small set of common development errors; implementing tools specifically to counter those errors should reduce vulnerabilities, particularly at the lower levels of assurance. Vulnerability identification tools are focused on finding common causes of vulnerability, and fuzz testing tools' approach also tends to find security vulnerabilities. In short, employing tools to focus on likely problems should significantly reduce the number and severity of vulnerabilities.

There is relatively little data on the speed or manpower required for tool-assisted evaluations as compared to manual evaluations. It is reasonable, however, to presume that evaluations supported by tools should require less manpower than a purely manual

approach. Secure Software, a company that performs tool-assisted security evaluations, reports an estimate of 3,000 lines of code per hour reviewed and analyzed when they use their (in-house) tools, versus 100 lines of code per hour if done manually (for what they believe are similar levels of scrutiny) [SECURE2004].

[VANDEVEN2005] reports on the experience of employing a single run-time countermeasure; they found that in the period from November 1, 2003 to August 11, 2004, there were 16 security issues with more severity than a Denial of Service problem and for which an exploit was made available. Out of these 16 exploits, 12 were countered by their countermeasure, yielding a success rate of 75% against unknown vulnerabilities (reducing their risk and impact).

Researchers are already working to improve the results of such tools. For example, [DACOSTA2003] found that that most vulnerabilities are clustered near inputs, a plausible hypothesis implied (but not proven) by previous tool developers' work. Thus, a tool that raises the risk level based on nearness to inputs should correctly identify what is the riskiest.

F.9 Implications

Tools are available, but the Common Criteria do not currently require their use. As a result, tools are often not used or required, even when it would be sensible to do so.

Tools could be used during the evaluation process itself, e.g., to perform source code scanning, fuzz testing, and standard test suites. However, this raises a fundamental question: How will these tools be developed and deployed? There are several options for development in each tool category, if they are to be used:

1. Select a specific commercial product for use. This has the advantage of simplicity and commercial support. However, if it is a commercial product, doing so will put competing products at a significant disadvantage, and any such selection is likely to be challenged. In practice, the costs of such products may be quite large (especially since, as a monopoly supplier, a vendor may take advantage of their status where they can). Any required tool essentially becomes part of a government mandate & a government regulation for production. Note also that vendors of such products tend to not reveal in detail their measurement criteria. As a result, this option would essentially cede the definition of security to a third-party commercial firm. This would also make it more difficult for firms to perform such testing ahead-of-time, since such products may be as expensive as a Common Criteria evaluation.
2. Select a set of commercial products for use. This option avoids putting competing products at a significant disadvantage. However, this also means that the measurement criteria will vary, depending on which product is used, greatly reducing the uniformity desired for the Common Criteria. And again, this option essentially cedes the definition of security to third parties.
3. NIAP-developed tools. The original plans for the NIAP included the intent to develop tools, which would counter the disadvantages of the first two approaches. The disadvantage here would be the costs of tool development and maintenance. On the positive side, the NIAP could freely release its own tools, greatly increasing the likelihood of widespread adoption (eliminating product vulnerabilities long before

they entered an evaluation, if they ever did). This would also be clearly fair and consistent. There are various cost-sharing methods that could be used to reduce somewhat the costs of initial development, and it is worth noting that evaluation costs are simply hidden in product costs (so the government would pay at least some money for the previous options too). Commercial vendors would be free to exploit those tools or their ideas, and could also develop tools that went beyond the NIAP tools.

To be practical, widely using tools ay require modifying lower EAL levels to require source code. Many tools require source code, and a significant number require the ability to rebuild an executable program from source code (to perform instrumentation). The current CC requires all source code at EAL5, with only a sample at EAL4, and nothing below EAL4. The updated CC is expected to require all source code at EAL4, but nothing below that. An alternative would be to require all source code (with build instructions) at EAL2 or 3. This will require intellectual property protections, but labs already make such arrangements for EAL4 and above, and there is little evidence that *vendors* have trouble with this. Vendors can choose which lab they believe will provide adequate protection for their property, and avoid those labs whose procedures are inadequate. In the end, it is the *code* that is executed, not documentation, and many customers are skeptical of evaluation processes that ignore the program actually being executed. Tools could enable at least partial evaluation of the actual code that is being executed.

Of course, the mere existence of tools and elimination of roadblocks is not enough; tools are not relevant unless they are used. Tools could be implemented in several ways:

1. The Common Criteria's testing (ATE) and vulnerability assessment (AVA) assurance classes could be modified (or interpreted by the NIAP) to specifically require certain kinds of tool use in certain circumstances (e.g., for certain product types and EALs).
2. The entry criteria for evaluation could be modified to require the use of certain kinds of tools that reduce the likelihood of vulnerabilities, especially at higher levels of assurance. These include build mechanisms (e.g., compiler options to detect or counter problems), environmental requirements (e.g., buffer overflow protections), the use of certain kinds of secure libraries, and so on.

PPs of some platforms could be modified to include mechanisms that reduce vulnerabilities of applications that run on those platforms. For example, operating system PPs could be modified to require support for a buffer overflow protection mechanism.

Annex G. Alternative Forms of Assurance

Several interviewees believed that alternative assurance methods are needed, especially to reduce costs (such as a "CC lite"). This is the case for organizations or situations that cannot afford to pay for evaluations, such as many small web applications, small businesses, and open source software (OSS) projects. Support for alternative assurance levels was strongest for use in lower assurance evaluations. Many believed that the NIAP evaluation would be strengthened if the alternative assurance methods were used to supplement the NIAP evaluation, with SSE, CMM®, and CMMI® specifically mentioned as examples of alternative assurance methods.

G.1 Other Assurance Methods

Examining documentation, along with some vulnerability analysis and functional testing, is certainly not the only way to gain assurance that a product is unlikely to contain vulnerabilities of certain kinds. Other aspects could be examined instead or in addition:

G.1.1 Source/Binary Code Review

These reviews could be manual or with tools.

G.1.2 Code Proofs.

This area needs research in formal methods.

G.1.3 Peer Review/Focused Code Review

This is one aspect of an overall development process evaluation.

G.1.4 Development Process

This examines all aspects of the development process, including quality assurance, defect tracking, etc.

G.1.5 Standard Security Test Suites

For many common application areas, such as firewalls and intrusion detection systems, it would be possible to create a standard security test suite for each area. For example; for firewalls it would be possible to create a standard set of tests that any firewall should withstand. One challenge is that such a test suite must be under constant improvement itself, since attackers continuously create new attacks.

G.1.6 Field Use with Few Reported Vulnerabilities

Although it is not a perfect indicator, few reported vulnerabilities on a product that has significant field use could provide some assurance. However, this presumes there are people who are searching for vulnerabilities, that those vulnerabilities are reported, and that those vulnerabilities are eventually acknowledged publicly. None of these assumptions are always true.

G.1.7 Other Evaluation Processes

Note there is already an evaluation process for cryptographic modules (FIPS-140). Other evaluation processes include DCID 6/3 PL5 and/or DITSCAP (soon to become DIACAP).

G.2 Other Constraints/Requirements

Other constraints/requirements may include the following:

G.2.1 No/little vendor money

Many small businesses and open source software projects cannot afford an independent evaluation as structured today. It may be valuable to devise assurance or evaluation processes that can be used when there is little or no money available, though the vendor does have some time available for some kind of low-assurance evaluation.

G.2.2 Potential for malicious developer or vendor

The CC evaluation process as currently designed presumes there are no malicious developers. For example, a vendor is allowed to determine what evidence is given to an evaluator; if an evaluator is given false information, he may reach a false conclusion.

G.3 Combinations

These issues and approaches can be combined in many ways.

Example 1:

Use a specified set of tools to search for the most common vulnerabilities in the source code, fixing problems found

Use a standard test suite (provided by the evaluation)

Use a CM process with a few simple requirements, (e.g., limiting who can make changes to the trusted product to authorized users and ensuring that users know exactly what they received)

Use a trusted delivery process including digitally signed executables

Evaluators could briefly check to ensure that these were done, taking no more than a few hours.

Example 2:

A different high-assurance evaluation might include these kinds of requirements:

Proof of correctness at the source code level

Peer review of all source code (at the line-by-line level)

8-hour developer training in developing secure software (not including formal methods, which would be handled separately), including requirements, design, implementation issues (including common implementation mistakes), and testing. This training must occur before the developer is allowed to create artifacts for the project.

The Common Criteria could be modified to include other assurance classes, even if they are not a part of EALs. This would at least increase understanding and it might also encourage use of other assurance approaches where they are appropriate.

However, one general complication with the Common Criteria is that although they allow product evaluations to “mix and match” assurance processes, in practice it is the EAL collections that are followed. In some cases, alternative practices might actually give more assurance than the processes required in any particular EAL package. The problem is that the CC drive most users toward accepting only a particular set of assurance processes (those in the EALs). This is particularly so since any assurance class not listed

in the CC (or listed beyond EAL4) will not be mutually recognized. This is not an easy problem to fix; it is often difficult to measure the amount of actual assurance supplied by different assurance processes and, as a result, it is difficult to determine when replacement of one by another is acceptable. However, this means that in practice, the flexibility of the CC in terms of assurance classes is often underutilized.

G.4 Options

1. Make no changes.
2. Relax requirements in the CC process (especially documentation).
3. Specifically identify alternatives to the NIAP process.
4. Specifically create and identify new alternatives to the NIAP process, especially for low-assurance evaluations.
5. Replace the NIAP process with an alternative process.
6. Combine new approaches for low assurance, and cost reducers for high assurance.

G.5 Recommendation

We recommend a cost effective alternative for low assurance evaluations (EAL3 and below). Key elements of this low assurance evaluation process include; process assurance checking for the developer, minimal functional assurance testing by a laboratory, and the screening of the code and execution products by a standard set of tools.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
25-08-15	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Summary of Review of the National Information Assurance Partnership (NIAP)	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
J. Katharine Burton, Patricia A. Cohen, Rick A. Harvey, Reginald N. Meeson, Michael S. Nash, Sarah H. Nash, Edward A. Schneider, William R. Simpson, Martin R. Stytz, David A. Wheeler	5e. TASK NUMBER BC-5-2382
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	P-5224 H15-000011

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Assistant Secretary of Defense for Networks and Information Integration (OASD/NII DIAP) Crystal Gateway 3, Suite 1100, Arlington, VA 22202	OASD/NII DIAP
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, unlimited distribution: 14 August 2006.

13. SUPPLEMENTARY NOTES

Project Leader: Gregory N. Larsen

14. ABSTRACT

This study was mandated by the National Strategy to Secure Cyberspace which requires the federal government to conduct a comprehensive review of the National Information Assurance Partnership (NIAP) to determine the extent to which it is adequately addressing the continuing problem of security flaws in commercial software products. The NIAP is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to provide technical leadership in the research and development of security-related information technology test methods and assurance techniques. The study reviewed the policy and requirements for cybersecurity, the current structure and functionality of the NIAP, and the expectations of the stakeholders. The study developed issues and recommendations and provided several options for pursuing cybersecurity programs that include all the elements necessary to establish an efficient and functional operational capability to strengthen the security of the software used in US systems and commercial software products.

15. SUBJECT TERMS

Information Assurance, Cybersecurity, National Information Assurance Partnership (NIAP), Software Security.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			OASD/NII DIAP
Unclassified	Unclassified	Unclassified	Unlimited	260	19b. TELEPHONE NUMBER (Include Area Code)